REDACTED PUBLIC VERSION OF COMPLAINT FILED UNDER SEAL WITH PERMISSION OF THE COURT BY ORDER DATED AUGUST 2, 2023, ECF 85

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

In re LastPass Data Security Incident Litigation	Case Number: 1:22-cv-12047-PBS Hon. Patti B. Saris **CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Hustle N Flow Ventures LLC, Amy Doermann, Ayana Looney, Dan LeFebvre, David Andrew, Erik Brook, Glenn Mulvenna, Hui Li, Joel Eagelston, Debt Cleanse Group Legal Services LLC, Josh Shi, Nathan Goldstein, Noah Bunag, R. Andre Klein, Sarb Dhesi, and Steven Carter ("Plaintiffs"), individually and on behalf of all others similarly situated (the "Class" or "Class Members"), bring this action against LastPass US LP ("LastPass") and GoTo Technologies USA, Inc. ("GoTo") (collectively, "Defendants"), seeking monetary damages, restitution, and/or injunctive relief. Plaintiffs and the Class make the following allegations upon personal knowledge and on information and belief derived from, among other things, investigation by their counsel and facts that are a matter of public record.

I. INTRODUCTION

1. Plaintiffs bring this lawsuit because LastPass failed at its only job—protecting users' most sensitive and personal information. As a company in the business of storing and managing login credentials, identities, and passwords—literally the "keys to the kingdom"—for more than 33 million users and 100,000 businesses worldwide, LastPass knew it was among the most attractive targets for cybercriminals. The breach (the "Data Breach") exposed users' highly

sensitive data, including names, billing addresses, email addresses, telephone numbers, IP addresses, and (most shocking) entire customer vaults, which store unencrypted data such as website URLs, alongside encrypted data, such as the customer's login name and password for those websites—websites with private financial and medical information included.[1]

2. This Data Breach has led to the exposure, misappropriation, and misuse of millions of users' information through fraud, identity theft, phishing scams, credit-stuffing attacks, and various other kinds of injury to Plaintiffs and Class Members; these victims deserve compensation.

3. LastPass is a successful subscription and "freemium"[2]-based identity and password management company, which markets and sells one-stop security for all the needs of today's internet consumer. LastPass offers consumers the ability to save all their login credentials, for a limitless number of websites, behind one, easy-to-use, "master" password, in addition to providing them a secure vault in which to store sensitive information and documents.

4. LastPass's product is security, and it markets its product to consumers and businesses by promising that its "first priority" is the "safeguarding [of] your data."[3] GoTo, the parent company of LastPass, similarly touts "industry-leading zero trust security" to keep information secure.[4]

5. But Defendants did not live up to their security promises.

---

[1] The information exposed in the Data Breach is referenced herein as PII, which typically refers to personally identifiable information. To be clear, information exposed in the breach includes that information, which was also never intended to become public, was sensitive, and should have been maintained in a secure, non-accessible manner.

[2] "Freemium" services are those which are based on a pricing strategy providing a basic service or product free-of-charge, but charging a premium for additional features, services, or goods that expand the functionality of the free version of software.

[3] "How LastPass Works" https://www.lastpass.com/how-lastpass-works (last accessed on July 18, 2023).

[4] GoTo Home Page, https://www.goto.com/ (last accessed July 17, 2023).

6. Defendants represented and marketed that they provided robust cybersecurity protections for consumers, including Plaintiffs and Class Members, but in reality their own security program was woefully inadequate. Defendants' unsound, vulnerable systems containing the valuable data described herein were an open invitation for a multi-step intrusion and exfiltration of valuable data by cybercriminals in the Data Breach, who have exploited this data to target LastPass's customers, including Plaintiffs and Class Members.

7. The value of the information stored through Defendants' services is recognized by several different constituencies. First, the value is recognized by LastPass, which can attribute its business model (and revenues) to the existence, preservation, and protection of this information. Second, the value is recognized by cybercriminals, who know that this type of data can be exploited for hacking, phishing scams, SIM swaps, and other forms of identity theft. They can also sell this data for other nefarious purposes. And third, the value is recognized by the public, including Plaintiffs and Class Members, whose data was stolen in the Data Breach and whose internet security has been permanently compromised.

8. Not long after the breach, Plaintiffs and Class Members were exposed to increased fraud and security threats involving the same type of data that they stored with LastPass. Plaintiffs have lost access to accounts that were only accessible through their password vaults,

9. Despite LastPass's supposed "commitment to transparency,"[5] neither it nor GoTo have provided Plaintiffs and Class Members with some of the most basic information about the Data Breach—such as when it began, and how long the breach persisted. This is significant because Plaintiffs and Class Members have no idea how long hackers have had their information,

[5] *Id.*

and what information has been exposed so that they may take further steps to protect it. And instead of providing fulsome notice to individuals who were impacted by the Data Breach, including Plaintiffs and Class Members, Defendants have downplayed and minimized the incident.

10. Defendants' unlawfully deficient data security and utter failure, even now, to honestly address the Data Breach has injured millions of their customers, including Plaintiffs and Class Members in this action.

II. PARTIES

A. Plaintiffs

1. Amy Doermann

11. Plaintiff Amy Doermann is an adult citizen of the State of New York residing in Beacon, New York.

12. Ms. Doermann first opened an account with LastPass through her employer, Truepic, Inc., in or around October 2018. Plaintiff opened another account with LastPass through another employer, Takeoff Agency, in or around January 2022. She used her LastPass accounts for both professional and personal purposes.

13. Ms. Doermann first learned of the Data Breach in or around April 2023. On that date, she was first informed of the Data Breach through a friend.

14. The information stored in Ms. Doermann's LastPass accounts included her login credentials to her work e-mail accounts and servers, login credentials to her personal online accounts, and confidential documents, such as tax forms containing her sensitive financial account information.

15. Ms. Doermann is a victim of the Data Breach. Her PII and other sensitive information was exposed in the Data Breach because she stored personal documents, financial account information, and login credentials in her Vault. Such information was within the

possession and control of Defendants at the time of the Data Breach. Consequently, Plaintiff's PII and other highly sensitive and confidential information was among the data accessed and exfiltrated by one or more unauthorized third parties in the Data Breach.

16. Subsequent to the Data Breach, and in addition to the injuries alleged above, Ms. Doermann also experienced actual identity theft and fraud, including three, fraudulent applications to open credit cards in her name between April and July of 2023, and a massive uptick in spam text messages and calls since the Data Breach purporting to be from businesses for which she maintained login credentials in her Vault.

17. Since the announcement of the Data Breach, Ms. Doermann has spent approximately 72 hours responding to the Data Breach. As a direct consequence of the Data Breach, Ms. Doermann spent time talking to her credit card company to ensure the credit card applications fraudulently submitted in her name were not successful; monitoring her accounts; and seeking legal counsel regarding her options for remedying or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured. The time spent dealing with the repercussions of the Data Breach is time Ms. Doermann otherwise would have spent on other activities, such as work or recreation.

18. Ms. Doermann plans to take additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her accounts for any unauthorized activity.

19. Ms. Doermann has spent approximately $750 responding to the Data Breach. As a direct consequence of the Data Breach, Plaintiff spent money on phone bills relating to her calls to credit card companies in response to the fraudulent credit card applications and on two sessions

of therapy to discuss how exposed and violated she felt because of the Data Breach, and the emotional distress she has related to the exposure of her PII.

20. Before the Data Breach, Ms. Doermann believed that Defendants used cutting-edge security practices to ensure that her Vault was a secure and safe place to store her sensitive and confidential information and PII based on promises made by Defendants on their website, which Ms. Doermann visited and read prior to creating her first account.

21. Ms. Doermann suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that she entrusted to Defendants—which was compromised in and as a result of the Data Breach.

22. Ms. Doermann suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and has ongoing anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling her PII and other highly sensitive and confidential information.

23. Ms. Doermann has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII and other sensitive and confidential information, in combination with her name, being placed in the hands of unauthorized third parties/criminals.

24. Ms. Doermann has a continuing interest in ensuring that her PII and other sensitive information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

2. Ayana Looney

25. Plaintiff Ayana Looney is an adult citizen of the State of California residing in Sacramento.

26. Ms. Looney first opened an account with LastPass on or around April 14, 2020, and enrolled in a Premium Plan for which she paid approximately $36 per year.

27. Ms. Looney first learned of the Data Breach on or around December 22, 2022. On that date, she received an email from her employer stating that Defendants had experienced a breach, but that her stored information was still encrypted.

28. The information stored in Ms. Looney's LastPass account included over 300 different login credentials and answers to security questions for online accounts, including her banking, investing, income tax, and retirement accounts, as well as information pertaining to multiple credit card accounts.

29. Ms. Looney is a victim of the Data Breach. Her PII and other sensitive information was exposed in the Data Breach. Such information was within the possession and control of Defendants at the time of the Data Breach. Consequently, Plaintiff's PII and other highly sensitive and confidential information was among the data accessed and exfiltrated by one or more unauthorized third parties in the Data Breach.

30. Subsequent to the Data Breach, and in addition to the injuries alleged above, Ms. Looney also experienced a sudden and drastic increase in spam messages, averaging around 20 each day, spam calls to her phone, and other suspicious phishing attempts purporting to be from businesses for which she maintained login credentials in his Vault.

31. Since the announcement of the Data Breach, Ms. Looney has spent approximately 45 hours responding to the Data Breach. As a direct consequence of the Data Breach, Ms. Looney spent time changing the passwords and login credentials stored in her Vault, monitoring her accounts, and seeking legal counsel regarding her options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured. The time

spent dealing with the repercussions of the Data Breach is time Plaintiff otherwise would have spent on other activities, such as work and/or recreation.

32. Ms. Looney plans to take additional time-consuming and necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her accounts for any unauthorized activity.

33. Before the Data Breach, Ms. Looney believed that Defendants used cutting-edge security practices to ensure that her Vault was a secure and safe place to store her sensitive and confidential information based on promises made by Defendants in their privacy policy, which Ms. Looney read when she signed up in 2020.

34. Ms. Looney did not receive the benefit of her bargain and expected the level of security that Defendants touted throughout their marketing materials. Had Ms. Looney known the truth about Defendants' security practices, she would not have paid for Defendants' services or would have paid less for them.

35. Ms. Looney suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that she entrusted to Defendants, which was compromised in and as a result of the Data Breach.

36. Ms. Looney suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has ongoing anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling her PII and other highly sensitive and confidential information.

37. Ms. Looney has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII and other

sensitive and confidential information, in combination with her name, being placed in the hands of unauthorized third parties/criminals.

38. Ms. Looney has a continuing interest in ensuring that her PII and other sensitive information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

3. Daniel LeFebvre

39. Plaintiff Daniel LeFebvre is an adult citizen of the State of Oklahoma residing in Tulsa.

40. Mr. LeFebvre first opened an account with LastPass in or around 2010 and enrolled in a Premium Plan, for which he paid approximately $25 to 30 per year.

41. Mr. LeFebvre first learned of the Data Breach on or around August 25, 2022. On that date, he received a notice from Defendants stating that there was a breach, but that his stored information was still encrypted, and that customer Vaults were unaffected.

42. Mr. LeFebvre stored login credentials to all his online accounts in his LastPass account, including to his banking and financial accounts, as well as credit card information and other sensitive information.

43. Mr. LeFebvre is a victim of the Data Breach. His PII and other sensitive information were exposed in the Data Breach. Such information was within the possession and control of Defendants at the time of the Data Breach. Consequently, Plaintiff's PII and other highly sensitive and confidential information was among the data accessed and exfiltrated by one or more unauthorized third parties in the Data Breach.

44. Since the announcement of the Data Breach, Mr. LeFebvre has spent approximately 225 hours responding to the Data Breach. As a direct consequence of the Data Breach, he spent time changing the passwords and login credentials stored in his Vault, verifying the legitimacy and

impact of the Data Breach, exploring credit monitoring and identity theft insurance options, monitoring his accounts, and seeking legal counsel regarding its options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured. The time spent dealing with the repercussions of the Data Breach is time Mr. LeFebvre otherwise would have spent on other activities, such as work and/or recreation.

45. Mr. LeFebvre plans to take additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his accounts for any unauthorized activity and changing passwords for accounts that haven't been changed since the Data Breach.

46. Mr. LeFebvre has spent approximately $450.00 responding to the Data Breach. As a direct consequence of the Data Breach, he purchased identity theft protection and additional security tools and subscribed to a new password manager service.

47. Before the Data Breach, Mr. LeFebvre believed that Defendants used cutting-edge security practices to ensure that his Vault was a secure and safe place to store his sensitive and confidential information based on promises made on their website.

48. Mr. LeFebvre did not receive the benefit of his bargain and expected the level of security that Defendants touted throughout their marketing materials. Had Mr. LeFebvre known the truth about Defendants' security practices, he would not have paid for Defendants' services or would have paid less for them.

49. Mr. LeFebvre suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendants, which was compromised in and as a result of the Data Breach.

50. Mr. LeFebvre suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has ongoing anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling his financial and other highly sensitive and confidential information.

51. Mr. LeFebvre has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his other sensitive and confidential information, in combination with his name, being placed in the hands of unauthorized third parties/criminals.

52. Mr. LeFebvre has a continuing interest in ensuring that his PII and other sensitive information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

4. David Andrew

53. Plaintiff David Andrew is an adult citizen of the State of Illinois residing in Skokie.

54. Mr. Andrew first opened an account with LastPass in or around December 2017 and enrolled in the Family Plan, for which he paid approximately $48 per year.

55. Mr. Andrew first learned of the Data Breach in or around August 2022 while reading the news online.

56. The information stored in Mr. Andrew's LastPass account included his login credentials to approximately 500 online accounts, including banking and financial accounts.

57. Mr. Andrew is a victim of the Data Breach. His PII and other sensitive information was exposed in the Data Breach. Such information was within the possession and control of Defendants at the time of the Data Breach. Consequently, Mr. Andrew's highly sensitive and confidential information was among the data accessed and exfiltrated by one or more unauthorized third parties in the Data Breach.

58. Since the announcement of the Data Breach, Mr. Andrew has spent approximately 40 hours responding to the Data Breach. As a direct consequence of the Data Breach, Plaintiff spent time changing the passwords and login credentials stored in his Vault, verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring his accounts, and seeking legal counsel regarding his options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured. The time spent dealing with the repercussions of the Data Breach is time Mr. Andrew otherwise would have spent on other activities, such as work and/or recreation.

59. Mr. Andrew plans to take additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his accounts for any unauthorized activity.

60. Mr. Andrew has spent approximately $39 responding to the Data Breach. As a direct consequence of the Data Breach, Plaintiff subscribed to a replacement password manager service for $38.49 per year.

61. Mr. Andrew suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendants, which was compromised in and as a result of the Data Breach.

62. Before the Data Breach, Mr. Andrew believed that Defendants used cutting-edge security practices to ensure that the Vault was a secure and safe place to store his sensitive and confidential information based on promises made by Defendants on their website, which he read in 2017, and which have remained consistent in relevant part at all times relevant thereto.

63. Mr. Andrew did not receive the benefit of his bargain and expected level of security that Defendants touted throughout their marketing materials. Had Mr. Andrew known the truth

about Defendants' security practices, he would not have paid for Defendants' services or would have paid less for them.

64. Mr. Andrew suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has ongoing anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling his highly sensitive and confidential information.

65. Mr. Andrew has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and other sensitive and confidential information, in combination with his name, being placed in the hands of unauthorized third parties/criminals.

66. Mr. Andrew has a continuing interest in ensuring that his PII and other sensitive information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

5. Erik Brook

67. Plaintiff Erik Brook is an adult citizen of the State of Illinois residing in Chicago. At the time Plaintiff Brook signed up for Last Pass, he was a citizen of the State of California residing in Hermosa Beach.

68. Mr. Brook first opened an account with LastPass in or around 2010 and enrolled in the Free Plan. In March of 2021 he enrolled in a Premium Family Plan, for which he paid approximately $37 per year.

69. Mr. Brook first learned of the Data Breach in or around December 2022. On that date, he received an email from Defendants stating that there was a breach, but that his stored information was still encrypted, and that customer Vaults were unaffected.

70. The information stored in Mr. Brook's LastPass Vault included his login credentials to numerous online websites, social media platforms, and financial accounts, as well as PII, including social security numbers for himself, his wife, and his children, and other highly-sensitive information.

71. Mr. Brook and his family are victims of the Data Breach. Their PII and other sensitive information was exposed in the Data Breach. Such information was within the possession and control of Defendants at the time of the Data Breach. Consequently, their PII and other highly sensitive and confidential information was among the data accessed and exfiltrated by one or more unauthorized third parties in the Data Breach.

72. Since the announcement of the Data Breach, Mr. Brook has spent approximately 30 hours responding to the Data Breach. As a direct consequence of the Data Breach, he spent time changing the passwords and login credentials stored in his Vault, verifying the legitimacy and impact of the Data Breach, ensuring his credit was frozen, monitoring his accounts, creating a new password management account with another company and transferring over his information, and seeking legal counsel regarding its options for remedying or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured. The time spent dealing with the repercussions of the Data Breach is time Mr. Brook otherwise would have spent on other activities, such as work and/or recreation.

73. Mr. Brook plans to take additional time-consuming and necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his accounts for any unauthorized activity.

74. Mr. Brook suffered actual injury in the form of damages to and diminution in the value of his and his families' PII—a form of intangible property that he entrusted to Defendants, which was compromised in and as a result of the Data Breach.

75. Before the Data Breach, Mr. Brook believed that Defendants used cutting-edge security practices to ensure that the Vault was a secure and safe place to store his sensitive and confidential information and PII, based on promises made by Defendants on their website and in an email from Defendants sent on August 20, 2019, which repeated Defendants' uniform marketing statements in relevant part.

76. Mr. Brook did not receive the benefit of his bargain and expected level of security that Defendants touted throughout their marketing materials. Had Mr. Brook known the truth about Defendants' security practices, he would not have paid for Defendants' services or would have paid less for them.

77. Mr. Brook suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has ongoing anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling his PII and other highly sensitive and confidential information.

78. Mr. Brook has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and other sensitive and confidential information, in combination with his name, being placed in the hands of unauthorized third parties/criminals.

79. Mr. Brook has a continuing interest in ensuring that his PII and other sensitive information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

6. Glenn Mulvenna

80. Plaintiff Glenn Mulvenna is an adult citizen of the State of Florida residing in Flagler Beach.

81. Mr. Mulvenna first opened an account with LastPass in or around January 2020 and enrolled in the Free Plan.

82. Mr. Mulvenna first learned of the Data Breach in November 2022 from an online news story.

83. The information stored in Mr. Mulvenna's LastPass Vault included his login credentials to online accounts, including banking and financial accounts, and other sensitive information.

84. Mr. Mulvenna is a victim of the Data Breach. His PII and sensitive information was exposed in the Data Breach. Such information was within the possession and control of Defendants at the time of the Data Breach. Consequently, Mr. Mulvenna's highly sensitive and confidential information was among the data accessed and exfiltrated by one or more unauthorized third parties in the Data Breach.

85. Since the announcement of the Data Breach, Plaintiff Mulvenna and/or his paid consultant have spent approximately 120 hours responding to the Data Breach. As a direct consequence of the Data Breach, Plaintiff and/or his paid consultant spent time changing the passwords and login credentials stored in his Vault, verifying the legitimacy and impact of the Data Breach, creating new accounts, [redacted], and seeking legal counsel regarding its options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured. The time spent dealing with the repercussions of the Data Breach is time Plaintiff otherwise would have spent on other activities, such as work and/or recreation.

86. Plaintiff Mulvenna plans to take additional time-consuming and necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his accounts for any unauthorized activity.

87. Plaintiff Mulvenna has spent approximately $6,000 to $9,000 responding to the Data Breach. As a direct consequence of the Data Breach, Plaintiff paid a consultant to perform the remedial actions described above.

88. Plaintiff Mulvenna suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendants, which was compromised in and as a result of the Data Breach.

89. Mr. Mulvenna has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has ongoing anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling his PII and other highly sensitive and confidential information.

90. Before the Data Breach, Mr. Mulvenna believed that Defendants used cutting-edge security practices to ensure that the Vault was a secure and safe place to store his sensitive and confidential information based on promises made by Defendants on their website.

91. Mr. Mulvenna has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and other sensitive and confidential information, in combination with his name, being placed in the hands of unauthorized third parties or criminals.

92. Mr. Mulvenna has a continuing interest in ensuring that his PII and other sensitive information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

7. Hui Li

93. Plaintiff Hui Li is an adult citizen of the State of Illinois residing in Chicago. At the time he first began using Defendant's services, Plaintiff Li was a citizen of Pennsylvania residing in Havertown.

94. Mr. Li first opened an account with LastPass on or around May 11, 2016, and enrolled in the Free Plan.

95. Mr. Li first learned of the Data Breach in August 2022 through online news. In December 2022 he received an email from Defendants stating that there was a breach, but that his stored information was still encrypted, and that customer Vaults were unaffected.

96. The information stored in Mr. Li's LastPass Vault included his name, email address, login credentials to multiple online accounts including banking and financial accounts, and other sensitive information.

97. Mr. Li is a victim of the Data Breach. His PII and sensitive information was exposed in the Data Breach. Such information was within the possession and control of Defendants at the time of the Data Breach. Consequently, Mr. Li's PII and other highly sensitive and confidential information was among the data accessed and exfiltrated by one or more unauthorized third parties in the Data Breach.

98. Since the announcement of the Data Breach, Mr. Li has spent approximately seven hours responding to the Data Breach. As a direct consequence of the Data Breach, Mr. Li spent time changing the passwords and login credentials stored in his Vault, verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, monitoring his accounts, and seeking legal counsel regarding his options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

The time spent dealing with the repercussions of the Data Breach is time Plaintiff otherwise would have spent on other activities, such as work and/or recreation.

99. Mr. Li plans to take additional time-consuming and necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his accounts for any unauthorized activity.

100. Mr. Li suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendants, which was compromised in and as a result of the Data Breach.

101. Before the Data Breach, Mr. Li believed that Defendants used cutting-edge security practices to ensure that the Vault was a secure and safe place to store his sensitive and confidential information based on promises made by Defendants in their privacy policy, which Mr. Li read when he first signed up in 2016.

102. Mr. Li suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has ongoing anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling his PII and other highly sensitive and confidential information.

103. Mr. Li has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and other sensitive and confidential information, in combination with his name, being placed in the hands of unauthorized third parties/criminals.

104. Mr. Li has a continuing interest in ensuring that his PII and other sensitive information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

8. Joel Eagelston

105. Plaintiff Joel Eagelston is an adult citizen of the State of Arizona residing in Fountain Hills, Arizona, where he has resided since April 2023. At the time of the Data Breach, he was residing in Scottsdale, Arizona.

106. Mr. Eagelston first opened an account with LastPass in or around October 2012 and enrolled in a subscription plan, for which he paid $12 per year.

107. Mr. Eagelston first learned of the Data Breach on or around September 2022. On that date, he received a notice from Defendants stating that there was a breach, but that his stored information was still encrypted, and that customer Vaults were unaffected.

108. The information stored in Mr. Eagelston's LastPass Vault included his login credentials to more than 250 online accounts.

109. Mr. Eagelston is a victim of the Data Breach. His PII and other sensitive information was exposed in the Data Breach because he stored login credentials in his Vault. Such information was within the possession and control of Defendants at the time of the Data Breach. Consequently, Plaintiff's highly sensitive and confidential information was among the data accessed and exfiltrated by one or more unauthorized third parties in the Data Breach.

110. Since the announcement of the Data Breach, Mr. Eagelston has spent approximately 20 to 30 hours responding to the Data Breach. As a direct consequence of the Data Breach, Plaintiff spent time changing the passwords and login credentials stored in his Vault, verifying the legitimacy and impact of the Data Breach, monitoring his accounts, and seeking legal counsel regarding his options for remedying or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured. The time spent dealing with the repercussions of the Data Breach is time Mr. Eagelston otherwise would have spent on other activities, such as work and/or recreation.

111. Mr. Eagelston plans to take additional time-consuming and necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his accounts for any unauthorized activity.

112. Before the Data Breach, Mr. Eagelston believed that Defendants used cutting-edge security practices to ensure that his Vault was a secure and safe place to store his sensitive and confidential information based on promises made by Defendants on their website.

113. Plaintiff did not receive the benefit of his bargain and expected the level of security that Defendants touted throughout their marketing materials. Had Plaintiff known the truth about Defendants' security practices, he would not have paid for Defendants' services or would have paid less for them.

114. Mr. Eagelston suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendants, which was compromised in and as a result of the Data Breach.

115. Mr. Eagelston suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has ongoing anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling his highly sensitive and confidential information.

116. Mr. Eagelston has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his sensitive information, in combination with his name, being placed in the hands of unauthorized third parties/criminals.

117. Mr. Eagelston has a continuing interest in ensuring that his PII and other sensitive information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

9. Josh Shi

118. Plaintiff Josh Shi is an adult citizen of the State of Illinois residing in Naperville.

119. Mr. Shi first opened an account with LastPass in or around 2017 and enrolled in a Premium Plan, for which he paid approximately $36 per year.

120. Mr. Shi first learned of the Data Breach in or around July 2022, when he was informed about the Data Breach through a friend in the cybersecurity industry.

121. The information stored in Mr. Shi's LastPass account included his and his wife's login credentials for their online accounts and financial accounts, notes relating to his business, and other sensitive information.

122. Mr. Shi and his wife are victims of the Data Breach. His wife's and his PII and sensitive information was exposed in the Data Breach. Such information was within the possession and control of Defendants at the time of the Data Breach. Consequently, Mr. Shi's PII and other highly sensitive and confidential information was among the data accessed and exfiltrated by one or more unauthorized third parties in the Data Breach.

123. Since the announcement of the Data Breach, Mr. Shi has spent approximately 45 hours responding to the Data Breach. As a direct consequence of the Data Breach, Mr. Shi spent time on the phone with his credit card company to remedy an unauthorized charge on his credit card, changing the passwords and login credentials stored in his Vault, verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, monitoring his accounts, and seeking legal counsel regarding his options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

The time spent dealing with the repercussions of the Data Breach is time Mr. Shi otherwise would have spent on other activities, such as work and/or recreation.

124. Mr. Shi plans to take additional time-consuming and necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his accounts for any unauthorized activity.

125. Mr. Shi suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendants, which was compromised in and as a result of the Data Breach.

126. Before the Data Breach, Mr. Shi believed that Defendants used cutting-edge security practices to ensure that the Vault was a secure and safe place to store his sensitive and confidential information based on promises made by Defendants in their agreement with Mr. Shi when he signed up for their services—representations that were consistent with Defendants' uniform representations and marketing materials, and in Defendants' marketing materials, which Mr. Shi read in 2017.

127. Mr. Shi did not receive the benefit of his bargain and expected level of security that Defendants touted throughout their marketing materials. Had Mr. Shi known the truth about Defendants' security practices, he would not have paid for Defendants' services or would have paid less for them.

128. Mr. Shi suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has ongoing anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling his PII and other highly sensitive and confidential information.

129. Mr. Shi has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and other sensitive and confidential information, in combination with his name, being placed in the hands of unauthorized third parties/criminals.

130. Mr. Shi has a continuing interest in ensuring that his PII and other sensitive and confidential information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

10. Nathan Goldstein

131. Plaintiff Nathan Goldstein is an adult citizen of the State of Massachusetts residing in Brighton.

132. Mr. Goldstein first opened an account with LastPass in or around February 2021 and enrolled in a Family Plan, for which he paid approximately $51 per year.

133. Mr. Goldstein first learned of the Data Breach on or around December 23, 2022. On that date, he received a notice from Defendants stating that there was a breach, but that his stored information was still encrypted, and that customer Vaults were unaffected.

134. The information stored in Mr. Goldstein's LastPass account included his name, email address, login credentials to over 170 online accounts, his vaccination card, and personal notes about his investments.

135. Mr. Goldstein is a victim of the Data Breach. His PII and other sensitive information was exposed in the Data Breach. Such information was within the possession and control of Defendants at the time of the Data Breach. Consequently, Mr. Goldstein's PII and other highly sensitive and confidential information was among the data accessed and exfiltrated by one or more unauthorized third parties in the Data Breach.

136. Subsequent to the Data Breach, and in addition to the injuries alleged above, Mr. Goldstein also experienced a massive uptick in phishing attempts and suspicious spam text messages, emails, and calls purporting to be from businesses for which he maintained login credentials in his Vault. Additionally, an unknown party attempted to take control of his Microsoft account, the login credentials to which were stored in his Vault.

137. Since the announcement of the Data Breach, Mr. Goldstein has spent approximately 30 hours responding to the Data Breach. As a direct consequence of the Data Breach, Mr. Goldstein spent time changing the passwords and login credentials stored in his Vault, verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, monitoring his accounts, and seeking legal counsel regarding his options for remedying or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured. The time spent dealing with the repercussions of the Data Breach is time Mr. Goldstein otherwise would have spent on other activities, such as work and/or recreation.

138. Mr. Goldstein plans to take additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his accounts for any unauthorized activity.

139. Mr. Goldstein suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendants, which was compromised in and as a result of the Data Breach.

140. Before the Data Breach, Mr. Goldstein believed that Defendants used cutting-edge security practices to ensure that his Vault was a secure and safe place to store his sensitive and confidential information based on promises made by Defendants.

141. Mr. Goldstein did not receive the benefit of his bargain and expected level of security that Defendants touted throughout their marketing materials. Had Mr. Goldstein known the truth about Defendants' security practices, he would not have paid for Defendants' services or would have paid less for them.

142. Mr. Goldstein suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendants, which was compromised in and as a result of the Data Breach.

143. Mr. Goldstein suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has ongoing anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling his PII and other highly sensitive and confidential information.

144. Mr. Goldstein has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, in combination with his name, being placed in the hands of unauthorized third parties/criminals.

145. Mr. Goldstein has a continuing interest in ensuring that his PII and other sensitive and confidential information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

11. Noah Bunag

146. Plaintiff Noah Bunag is an adult citizen of the State of California residing in South San Francisco.

147. Mr. Bunag first opened an account with LastPass in or around 2012 and enrolled in the Free Plan.

148. Mr. Bunag first learned of the Data Breach on or around March 2, 2023. On that date, he learned about the Data Breach via an online news report. Subsequently, he received a notice via email from the Defendant in or around May 2023.

149. The information stored in Mr. Bunag's LastPass account included his name, address, phone number, and his Social Security Number, as well as login credentials to online accounts including banking and financial accounts.

150. Mr. Bunag is a victim of the Data Breach. His sensitive information was exposed in the Data Breach because he stored personal documents, PII, financial account information, and login credentials in Defendants' Vault. Such information was within the possession and control of Defendants at the time of the Data Breach. Consequently, Mr. Bunag's PII and other highly sensitive and confidential information was among the data accessed and exfiltrated by one or more unauthorized third parties in the Data Breach.

151. Subsequent to the Data Breach, and in addition to the injuries alleged above, Mr. Bunag also experienced actual identity theft and fraud, including a credit card account that was applied for under his name in January 2023 as well as an increase in phishing attempts via text messages and emails.

152. Mr. Bunag, has already been notified by Credit Karma and Experian that his information compromised in the Data Breach is now being sold on the dark web. Additionally, Plaintiff's loan application was denied due to a history of too many hard credit inquiries; there had been twenty-two hard inquiries, only three of which were attributable to Plaintiff.

153. Since the announcement of the Data Breach, Mr. Bunag has spent approximately 25 hours responding to the Data Breach. As a direct consequence of the Data Breach, he spent time changing the passwords and login credentials stored in his Vault, verifying the legitimacy and

impact of the Data Breach, replacing his credit cards, self-monitoring his accounts, and seeking legal counsel regarding his options for remedying or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured. The time spent dealing with the repercussions of the Data Breach is time Mr. Bunag otherwise would have spent on other activities, such as work or recreation.

154. Mr. Bunag plans to take additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his accounts for any unauthorized activity.

155. Mr. Bunag has spent hundreds of dollars responding to the Data Breach, including cancelling and resubscribing to online accounts and having multiple credit cards cancelled and reissued.

156. Mr. Bunag suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendants, which was compromised in and as a result of the Data Breach.

157. Mr. Bunag suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has ongoing anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling his PII and other highly sensitive and confidential information.

158. Mr. Buang has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and other sensitive and confidential information, in combination with his name, being placed in the hands of unauthorized third parties/criminals.

159. Mr. Buang has a continuing interest in ensuring that his PII and other sensitive and confidential information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

12. R. Andre Klein

160. Plaintiff R. Andre Klein is an adult citizen of the State of New York residing in Willsboro.

161. Mr. Klein first opened an account with LastPass on or around May 11, 2011, and enrolled in a Premium Plan, for which he paid approximately $12 per year starting in 2012 and $24 per year starting in 2018.

162. Mr. Klein first learned of the Data Breach on or around August 25, 2022. On that date, he received an email from Defendants stating that there was a breach, but that his stored information was still encrypted, and that customer Vaults were unaffected.

163. The information stored in Mr. Klein's LastPass Vault included his name, email address, login credentials to at least 350 online accounts including banking and financial accounts, and PII, including images of his and four other family members' social security cards, passports, and driver's licenses.

164. Mr. Klein and his family are victims of the Data Breach. His and his family's PII and other sensitive information was exposed in the Data Breach. Such information was within the possession and control of Defendants at the time of the Data Breach. Consequently, Mr. Klein's PII and other highly sensitive and confidential information was among the data accessed and exfiltrated by one or more unauthorized third parties in the Data Breach.

165. Since the announcement of the Data Breach, Mr. Klein has spent approximately 120 hours responding to the Data Breach. As a direct consequence of the Data Breach, Plaintiff spent time changing passwords, two factor authentication seeds, and login credentials for most or

all of the 350 online accounts saved in his Vault, closing compromised financial accounts and opening replacement accounts, cancelling and replacing compromised credit cards, and driving approximately 320 miles to close and reopen compromised bank accounts and replace compromised ATM cards. This time has been lost forever and cannot be recaptured. The time spent dealing with the repercussions of the Data Breach is time Mr. Klein otherwise would have spent on other activities, such as work or recreation.

166. Mr. Klein plans to take additional time-consuming and necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his accounts for any unauthorized activity.

167. Mr. Klein suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendants, which was compromised in and as a result of the Data Breach.

168. Before the Data Breach, Mr. Klein believed that Defendants used cutting-edge security practices to ensure that the Vault was a secure and safe place to store his sensitive and confidential information and PII, based on promises made by Defendants in their website, which he read in 2011. Mr. Klein did not receive the benefit of his bargain and expected the level of security that Defendants touted throughout their marketing materials. Had Mr. Klein known the truth about Defendants' security practices, he would not have paid for Defendants' services or would have paid less for them.

169. Mr. Klein suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has ongoing anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling his PII and other highly sensitive and confidential information.

170. Mr. Klein has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and other sensitive and confidential information, in combination with his name, being placed in the hands of unauthorized third parties or criminals.

171. Mr. Klein has a continuing interest in ensuring that his PII and other sensitive information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

13. Sarbjit Dhesi

172. Plaintiff Sarbjit Dhesi is an adult citizen of the State of California residing in San Ramon.

173. Mr. Dhesi first opened an account with LastPass in 2012 and enrolled in a Premium Plan. In 2021, Mr. Dhesi upgraded to a Family Plan for which he paid approximately $24 per year.

174. Plaintiff first learned of the Data Breach in or around December 2022. On that date, he received an email from Defendants stating that there was a breach, but that his stored information was still encrypted, and that customer Vaults were unaffected.

175. Mr. Dhesi is a victim of the Data Breach. His PII and other sensitive information was exposed in the Data Breach. Such information was within the possession and control of Defendants at the time of the Data Breach. Consequently, Mr. Dhesi's PII and other highly sensitive and confidential information was among the data accessed and exfiltrated by one or more unauthorized third parties in the Data Breach.

176. Since the announcement of the Data Breach, Mr. Dhesi has spent approximately 24 hours responding to the Data Breach. As a direct consequence of the Data Breach, he spent time changing the passwords and login credentials stored in his Vault, verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options,

monitoring his accounts, and seeking legal counsel regarding his options for remedying or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured. The time spent dealing with the repercussions of the Data Breach is time Mr. Dhesi otherwise would have spent on other activities, such as work and/or recreation.

177. Mr. Dhesi plans to take additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his accounts for any unauthorized activity.

178. Mr. Dhesi has spent approximately $285 responding to the Data Breach. As a direct consequence of the Data Breach, [redacted], which cost $225 and switched to a new password manager, which costs $59.85 per year.

179. Before the Data Breach, Mr. Dhesi believed that Defendants used cutting-edge security practices to ensure that the Vault was a secure and safe place to store his sensitive and confidential information based on promises made by Defendants on their website since he signed up in 2010.

180. Mr. Dhesi did not receive the benefit of his bargain and expected the level of security that Defendants touted throughout their marketing materials. Had Mr. Dhesi known the truth about Defendants' security practices, he would not have paid for Defendants' services or would have paid less for them.

181. Mr. Dhesi suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has ongoing anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling his PII and other highly sensitive and confidential information.

182. Mr. Dhesi has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and other sensitive and confidential information, in combination with his name, being placed in the hands of unauthorized third parties/criminals.

183. Mr. Dhesi has a continuing interest in ensuring that his PII and other sensitive and confidential information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

14. Steven Carter

184. Plaintiff Steven Carter is an adult citizen of the State of New York residing in Brooklyn.

185. Mr. Carter first opened an account with LastPass in or around 2018 and enrolled in a Premium Plan, for which he paid approximately $24 per year.

186. Mr. Carter first learned of the Data Breach in or around September 2022 when he read about it in technology-related media.

187. The information stored in Mr. Carter's LastPass account included his name, email address, login credentials to 286 online accounts including banking and financial accounts, and PII, including images of his social security card.

188. Mr. Carter is a victim of the Data Breach. His PII and other sensitive information was exposed in the Data Breach because he stored personal documents and financial account information and login credentials in his Vault. Such information was within the possession and control of Defendants at the time of the Data Breach. Consequently, Mr. Carter's PII and other highly sensitive and confidential information was among the data accessed and exfiltrated by one or more unauthorized third parties in the Data Breach.

189. Subsequent to the Data Breach, and in addition to the injuries alleged above, Mr. Carter also experienced actual identity theft and fraud, including multiple applications for payday loans submitted in his name, multiple unauthorized charges to his credit cards, and an increase in phishing attempts via text message and emails purporting to be from businesses for which he maintained login credentials in his Vault. Additionally, Mr. Carter has already been notified by Credit Karma that his information compromised in the Data Breach is now being sold on the dark web.

190. Since the announcement of the Data Breach, Mr. Carter has spent hundreds of hours responding to the Data Breach. As a direct consequence of the Data Breach, Mr. Carter spent time changing the passwords and login credentials stored in his Vault, verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, monitoring his accounts, and seeking legal counsel regarding his options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured. The time spent dealing with the repercussions of the Data Breach is time Mr. Carter otherwise would have spent on other activities, such as work or recreation.

191. Mr. Carter plans to take additional time-consuming and necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his accounts for any unauthorized activity.

192. Mr. Carter has spent approximately $250 responding to the Data Breach. As a direct consequence of the Data Breach, Plaintiff has had to pay for credit monitoring.

193. Mr. Carter suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendants, which was compromised in and as a result of the Data Breach.

194. Before the Data Breach, Mr. Carter believed that Defendants used cutting-edge security practices to ensure that the Vault was a secure and safe place to store his sensitive and confidential information and PII, based on promises made by Defendants verbally. Mr. Carter did not receive the benefit of his bargain and expected level of security that Defendants touted throughout their marketing materials. Had Mr. Carter known the truth about Defendants' security practices, he would not have paid for Defendants' services or would have paid less for them.

195. Mr. Carter suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has ongoing anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling his PII and other highly sensitive and confidential information.

196. Mr. Carter has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and other sensitive and confidential information, in combination with his name, being placed in the hands of unauthorized third parties/criminals.

197. Mr. Carter has a continuing interest in ensuring that his PII and other sensitive and confidential information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

15. Debt Cleanse Group Legal Services LLC

198. Plaintiff Debt Cleanse Group Legal Services LLC ("Debt Cleanse") is a Delaware limited liability company with its principal place of business in Chicago, Illinois.

199. Debt Cleanse first opened an account with LastPass in or around 2015 and enrolled in a Business Plan, for which it paid approximately $120.00 per month.

200. Debt Cleanse first learned of the Data Breach in or around February 2023. On that date, Debt Cleanse received a notice from Defendants stating that there was a breach, but that the stored information was still encrypted, and that customer Vaults were unaffected.

201. The information stored in Debt Cleanse's LastPass account included login credentials to 500 online accounts, including banking and financial accounts. Debt Cleanse's employees also used LastPass to store their login credentials and other sensitive information.

202. Debt Cleanse and its employees are victims of the Data Breach. Their PII and other sensitive and confidential information was exposed in the Data Breach. Such information was within the possession and control of Defendants at the time of the Data Breach. Consequently, the highly sensitive and confidential information of Debt Cleanse and its employees was among the data accessed and exfiltrated by one or more unauthorized third parties in the Data Breach.

203. Since the announcement of the Data Breach, Debt Cleanse's employees have spent approximately 50 hours responding to the Data Breach. As a direct consequence of the Data Breach, Debt Cleanse's employees spent time changing the passwords and login credentials stored in its Vault, verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, and seeking legal counsel regarding its options for remedying or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured. The time spent dealing with the repercussions of the Data Breach is time Debt Cleanse's employees otherwise would have spent on other activities.

204. Debt Cleanse must take additional time-consuming and necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing its accounts for any unauthorized activity.

205. Debt Cleanse has spent approximately $10,000 responding to the Data Breach. As a direct consequence of the Data Breach, Debt Cleanse has had to expend money on both internal and external costs, including but not limited to having to spend time to change passwords, transition all systems and employees to a new password product, and the retention of a third-party security firm to conduct independent investigations into the unauthorized access into at least one account that was compromised in the Data Breach.

206. Before the Data Breach, Debt Cleanse believed that Defendants used cutting-edge security practices to ensure that the Vault was a secure and safe place to store sensitive and confidential information based on promises made by Defendants verbally—using representations consistent with their uniform security representations, on their website, in their marketing materials, and in the contract with Debt Cleanse, which Debt Cleanse read in connection with subscribing to Defendants' services in 2015.

207. Debt Cleanse did not receive the benefit of its bargain and expected level of security that Defendants touted throughout their marketing materials. Had Debt Cleanse known the truth about Defendants' security practices, it would not have paid for Defendants' services or would have paid less for them.

208. Debt Cleanse's employees have suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has ongoing anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling their PII and other highly sensitive and confidential information.

209. Debt Cleanse and its employees have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their

PII and other sensitive and confidential information, in combination with their names, being placed in the hands of unauthorized third parties/criminals.

210. Debt Cleanse has a continuing interest in ensuring that its employees' PII and other sensitive information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

16. Hustle N Flow Ventures, LLC

211. Plaintiff Hustle N Flow Ventures, LLC ("HNF") is a Florida limited liability company organized and headquartered in West Palm Beach, Florida.

212. HNF opened an account with LastPass in or around November 2021 and enrolled in the Business Plan, for approximately $100-200 per year.

213. HNF first learned of the Data Breach in or around August 2022 via a news article.

214. The information stored in HNF's LastPass Vault included its employees' and clients' login credentials to approximately 20 online accounts, including banking and financial accounts. HNF's contractors also used LastPass to store their login credentials.

215. HNF and HNF's employees, clients, and contractors are victims of the Data Breach. Their PII and other sensitive information was exposed in the Data Breach. Such information was within the possession and control of Defendants at the time of the Data Breach. Consequently, their PII and other highly sensitive and confidential information was among the data accessed and exfiltrated by one or more unauthorized third parties in the Data Breach.

216. HNF has spent over a dozen hours responding to the Data Breach. Additionally, as a direct consequence of the Data Breach, HNF's employees spent time changing the passwords and login credentials stored in HNF's Vault, monitoring its accounts, and seeking legal counsel regarding its options for remedying or mitigating the effects of the Data Breach. This time has

been lost forever and cannot be recaptured. The time spent dealing with the repercussions of the Data Breach is time HNF's employees otherwise would have spent on other activities.

217. HNF's leadership and employees must take additional time-consuming, necessary steps to further mitigate the harm caused by the Data Breach, including continually reviewing accounts for any unauthorized activity.

218. Before the Data Breach, HNF believed that Defendants used cutting-edge security practices to ensure that the Vault was a secure and safe place to store its sensitive and confidential information and PII based on promises made by Defendants on their website, which HNF read prior to creating HNF's account, and verbally, in a call with one of Defendants' marketing or sales agents, which repeated their standard marketing language.

219. HNF did not receive the benefit of its bargain and expected level of security that Defendants touted throughout their marketing materials. Had Plaintiff known the truth about Defendants' security practices, it would not have paid for Defendants' services or would have paid less for them.

220. HNF has a continuing interest in ensuring that its PII and other sensitive information, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

B. Defendants

221. Defendant LastPass US LP ("LastPass") is a limited partnership organized under the laws of Delaware, with its principal place of business at 333 Summer Street, Boston, Massachusetts 02210. On information and belief, LastPass is still controlled by two private equity firms: Francisco Partners and Evergreen Coast Capital Corp, which also control Defendant GoTo Technologies USA, Inc.

222. Defendant GoTo Technologies USA, Inc. ("GoTo"), formerly known as LogMeIn, is a Delaware corporation with its principal place of business in Boston, Massachusetts. GoTo is a LastPass affiliate authorized to provide and support LastPass services. GoTo provides software and cloud-based remote work tools. GoTo, then known as LogMeIn, acquired LastPass in 2015 and later rebranded as GoTo in 2022.

III. SEALED ALLEGATIONS AS TO ADDITIONAL INJURIES

223. Beyond the other allegations in this Complaint, Plaintiffs have experienced specific fraud reasonably related to the Data Breach. Plaintiffs' specific allegations of fraud have been sealed to protect them from additional exploits by threat actors and cybercriminals.

[redacted]

[redacted]

[redacted]

IV. JURISDICTION AND VENUE

231. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because at least one member of each Class and Subclass, as defined below, is a citizen of a different state than LastPass.

232. This Court has personal jurisdiction over LastPass because LastPass maintains its principal place of business in this District, has sufficient minimum contacts with this District and has purposefully availed itself of the privilege of doing business in this District, such that it could reasonably foresee litigation being brought in this District.

233. This Court has personal jurisdiction over GoTo because GoTo maintains its principal place of business in this District, has sufficient minimum contacts with this District and has purposefully availed itself of the privilege of doing business in this District, such that it could reasonably foresee litigation being brought in this District.

234. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because the Defendants' principal places of business are located in this District and a substantial part of the events or omissions giving rise to the claims occurred in, was directed to, and/or emanated from this District.

V. STATEMENT OF FACTS

A. LastPass and GoTo Offered the Illusion of Protection from Hackers, While Failing to Engage Strong Cybersecurity Measures Themselves

235. LastPass is a company that brings to the market only one product: security in an increasingly online world.

236. Based upon information and belief, LastPass is controlled by GoTo, which influences and controls the security standards LastPass adopts and representations LastPass makes.

237. Founded in 2008, LastPass describes itself as "leading the way in password security and identity management for personal and business digital safety," "a pioneer in cloud security technology," and claims it "provides award-winning password and identity management solutions that are convenient, effortless, and easy to manage." According to LastPass, the company "values users' privacy and security, so your sensitive information is always hidden—even from us."[6]

238. LastPass offers a suite of services through its primary product, its password manager product, including a "password generator" (which automatically generates "secure

[6] About LastPass, https://www.lastpass.com/company/about-us (last accessed July 13, 2023).

passwords" for users),[7] dark web monitoring (which automatically monitors and detects whether a user's information has been exposed online),[8] and a "security dashboard," which provides a central place to check the "health and safety of your accounts."[9] Each of these services is described in more detail below, but LastPass primarily makes revenue through the provision of password manager services, provided through freemium and subscription plans to individual consumers, "family plan" groups of consumers, and corporate clients.

239. LastPass describes the "password manager" service it offers as follows:[10]

> A password manager is a tool that does the work of creating, remembering and filling in passwords. Simply log into an online account for the first time and LastPass will store your username and password so every time you go back your credentials will be filled in automatically.

240. Aside from every login and password that each consumer might link to LastPass, LastPass also stores "personal information," which it describes as "your most valuable documents", such as "passport, credit cards, social security, etc."[11]

241. LastPass suggests that its customers, including Plaintiffs and Class Members, protect their "Banking," "Email," and "Social Media" accounts with the LastPass password manager, effectively encouraging customers to link all their most sensitive accounts to the LastPass password manager.[12]

---

[7] Password Generator, https://www.lastpass.com/features/password-generator (last accessed on Jan. 10, 2023).

[8] Dark Web Monitoring, https://www.lastpass.com/features/dark-web-monitoring (last accessed on Jan. 10, 2023).

[9] Digital Security Dashboard, https://www.lastpass.com/features/security-dashboard (last accessed on Jan. 10, 2023).

[10] The Best Free Password Manager, https://www.lastpass.com/password-manager (last accessed on Jan. 10, 2023).

[11] *Id.*

[12] *Id.*

242. Like other entities that host such information, LastPass knew that hosting such information made it an attractive target for cybercriminals.

243. Indeed, GoTo was also aware of the attractive target for cybercriminals; having also been the target of one or more data breaches.[13]

244. LastPass offered the illusion of protection to its customers, including Plaintiffs and Class Members, through its password manager service, which would provide them two distinct, but interlinked, benefits: (1) they would not have to remember dozens, or even hundreds of login names and passwords, allowing their passwords to be more complex (and therefore harder to crack); and (2) they could manage all those logins and passwords from a single login and password with LastPass, which would follow them around the internet via a browser extension or mobile app. LastPass offers this service to make "[f]orgetting passwords . . . a thing of the past." According to its website, through either a browser add-on extension or a mobile device app, a user can allow LastPass to save login credentials and passwords under one "master password," which users, including Plaintiffs and Class Members, can employ to funnel the correct login and password details to any website they visit on their device.[14]

245. Emphasizing how necessary and essential its services are, LastPass offers this dire warning: "Doing nothing could mean losing everything. That's why password security has never been more critical for individuals and businesses."[15] To prevent this dire outcome, LastPass

---

[13] *See, e.g.*, Our Response to a Recent Security Incident, https://www.goto.com/blog/our-response-to-a-recent-security-incident (updated Apr. 20, 2023).

[14] The Best Free Password Manager, https://www.lastpass.com/password-manager (last accessed on Jan. 10, 2023).

[15] *Id.*

encourages potential customers to subscribe to LastPass's "Password Vault" service, which LastPass describes as "like a physical safe but for your online valuables."[16]

246. LastPass offers its customers, including Plaintiffs and Class Members, the ability to store "*everything you've saved* including passwords, secure notes, and credit card information," and even offers a "browser extension" which LastPass claims "will automatically capture account passwords as you enter them on every website."[17]

247. Customers, including Plaintiffs and Class Members, secured their Password Vaults, in which they stored their logins and passwords (hereafter "credentials") for an unlimited number of websites, as well as their credit card information, social security numbers, and other sensitive information and/or PII, with a "master password," which LastPass claims "are never sent to LastPass's servers, and are never accessible by LastPass."[18]

248. In addition to storing credentials to other websites, LastPass encourages customers to entrust the corporation with their highly sensitive PII, including Social Security numbers and driver's license numbers, promising that all will be held "securely."[19] Indeed, LastPass explicitly promises to safeguard customers' "most valuable documents," including passports, credit cards, and social security information.[20]

---

[16] Password Vault Software, https://www.lastpass.com/features/password-vault (last accessed July 13, 2023).

[17] *Id.* (emphasis added).

[18] *Id.*

[19] *Id.*

[20] *Id.*

249. LastPass also advertises to its customers the ability to store payment information in a "digital wallet" and to provide "dark web monitoring" that includes monitoring third-party data breaches of customer accounts, thereby promising to keep customers "informed and secure."[21]

250. LastPass purported to provide this service to both businesses and individual consumers by offering subscription-based password management through both enterprise and individual consumer accounts.

251. In addition, LastPass offered this service for free: a customer of LastPass can use the LastPass password vault system without paying any money.[22]

252. LastPass also offers family plans, allowing a consumer to "[s]ecure your entire family — your spouse, parents, kids and more" for a low monthly rate.[23]

253. LastPass offered company-wide password security to its enterprise clients, while also offering individual consumers the ability to manage all their sensitive information and login credentials from one convenient platform.

254. LastPass made this possible to its customers, including Plaintiffs and Class Members, by providing them with a "vault," or a single storage space only accessible through LastPass, in which LastPass claimed Plaintiffs and the Class could store their credentials, sensitive PII, and various other forms of sensitive documents and information, including but not limited to cryptocurrency keys, social security numbers, financial account numbers, and other forms of sensitive information.

---

[21] *Id.*

[22] LastPass Premium vs. Free, https://www.lastpass.com/pricing/lastpass-premium-vs-free (last accessed July 13, 2023).

[23] LastPass Families, https://www.lastpass.com/products/family-password-manager (last accessed July 13, 2023).

255. The consumer demand for this data privacy and security service is strong: LastPass's published user statistics boast over 33 million individual customers and over 100,000 businesses as registered users.[24]

256. LastPass in part created this market through its representations.

257. LastPass similarly boasts of the numerous awards it has received from cybersecurity experts.[25]

258. LastPass explicitly markets its password management service as essential, because "Data breaches are on the rise," and "password security has never been more critical for individuals and businesses" because—according to LastPass—over 80% of data breaches are caused by weak, reused, or stolen passwords.[26]

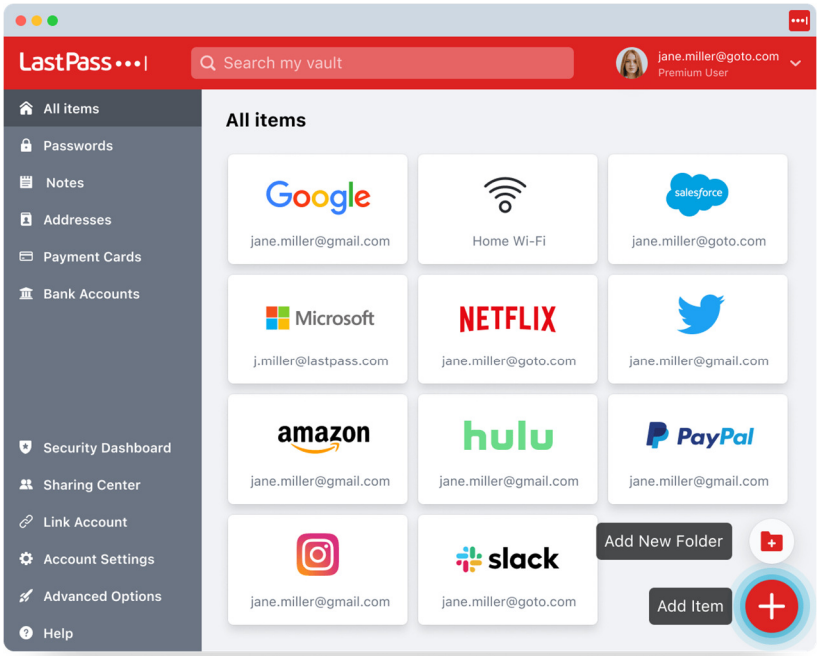
[24] About LastPass, https://www.lastpass.com/company/about-us (last accessed July 13, 2023).

[25] Security, https://www.lastpass.com/security (last accessed July 13, 2023).

[26] About Us, https://www.lastpass.com/company/about-us (last accessed July 13, 2023).

259. To combat this, LastPass instructs customers to think of their vault "like a physical safe but for your online valuables."[27] Although LastPass is a cloud-based security system, LastPass boasts the security of the program as unmatched because it employs "local-only encryption."[28]

260. Users can use their password manager vault to manage usernames, photographs, email credentials, websites visited, passwords, notes, addresses, payment cards, and linked bank accounts.[29]



[27] Password Vault Software, https://www.lastpass.com/features/password-vault (last accessed July 13, 2023).

[28] *Id.*

[29] How to Use LastPass Password Manager, https://www.lastpass.com/how-lastpass-works (last accessed July 13, 2023).

261. The company assures customers that their "data is kept secret, even from us"[30] and that "[o]nly you can unlock [your vault] with your master password."[31] Indeed, LastPass goes as far as stating customers may, in using LastPass, "make it nearly impossible for hackers to access your accounts."[32]

262. Consistent with this, Section 4.2 of LastPass's Terms of Service for Personal Use states that LastPass "ha[s] implemented and maintain[s] appropriate organizational, administrative, and technical safeguards designed to protect your Content against any unauthorized access, loss, misuse, or disclosure."[33]

263. Further explaining their "foundation of security," LastPass's website also claims that it employs a "transparent incident response" and that its "team reacts swiftly to reports of bugs or vulnerabilities and communicates transparently with our community."[34]

264. LastPass also offers enterprise accounts to businesses, enticing corporate customers with the ability to protect their systems despite their employees', or customers', use of third-party apps.[35] As an ominous warning to their potential corporate customers, LastPass states that "68% of workers put their employers at risk by using weak or reused passwords," and, perhaps

---

[30] Why LastPass?, https://www.lastpass.com/security/zero-knowledge-security (last accessed March 6, 2023).

[31] *Id.*

[32] *Id.*

[33] LastPass Terms of Service, https://www.lastpass.com/legal-center/terms-of-service/personal (last accessed July 13, 2023).

[34] A Foundation of Security, https://www.lastpass.com/security/zero-knowledge-security (last accessed Feb. 13, 2023).

[35] Scale Password Protection across Your Enterprise, https://www.lastpass.com/solutions/enterprise-password-management (last accessed on July 13, 2023) ("End users continue to adopt and share cloud-based apps outside IT's control. Protect all apps, end users, and data with pervasive password management.").

prophetically given the Data Breach, "55% of enterprises risk data breaches by not internally managing passwords."[36]

265. Eager to flex its competitive muscle, LastPass boasts that over "100,000 forward-thinking businesses" already use LastPass's services, including Patagonia and Yelp.[37]

266. LastPass lulls customers into a false sense of security that it will proactively and affirmatively secure customer PII. It styles these services as "auto-pilot for all your passwords" that provides "peace of mind everywhere you go"[38] and assures customers that "[s]afeguarding your data is what we do, with proactive security and reliability as cornerstones of our mission."[39]

267. This false sense of security ultimately doomed millions of LastPass customers to having their most personal, private, and sensitive information stolen.

B. Defendants Failed to Comply with Industry and Regulatory Standards, Despite Previous Security Issues

268. Millions of individuals, through individual accounts, shared accounts, and enterprise accounts, have shared their valuable data, including login credentials, passwords, and related names, email addresses, IP addresses, phone numbers, and the URLs of websites with which they maintain logins with LastPass based on the ordinary, reasonable understanding that their information would be handled and maintained with appropriate safety standards—the very services that LastPass was engaged to and promised to perform.

---

[36] *Id.*

[37] *Id.*

[38] Password management from anywhere, https://www.lastpass.com (last accessed March 6, 2023).

[39] Zero-Knowledge Encryption & Security Model, https://www.lastpass.com/security/zero-knowledge-security (last accessed July 13, 2023). Defendant GoTo previously represented that it used a "zero trust" model; however, that language has now been removed from its website.

269. LastPass knows that the customer PII entrusted to it is highly sensitive and highly valuable to hackers. Regarding banking, cryptocurrency, and other financial resources, the corporation stated that "extra precautions are essential when it comes to protecting [customers'] money."[40] With regard to protecting email account credentials, LastPass called email the "hub" of online life and the "gateway" to performing password resets, admonishing that customers "need to protect it."[41] When addressing the protection of social media account credentials, LastPass notes that social media sites contain personal information that "hackers love." [42]

270. In acknowledgement of the value of PII to its customers and to potential hackers, LastPass makes a "pledge" to its customers, including that it will protect customer data by making security its "top priority," communicate with customers regarding "security-related incident[s]," and that its services will be "effortless to manage." [43]

271. In support of its offers of safety and security in its product, LastPass claims that "security is our number one priority" and that its cybersecurity protections are "SOC 2 Type II compliant."[44]

272. Despite these acknowledgments and promises, LastPass failed to adopt and comply with industry standard regulations that may have limited the extent of, or prevented entirely, the Data Breach.

---

[40] The Best Free Password Manager, https://www.lastpass.com/password-manager (last accessed July 14, 2023).

[41] *Id.*

[42] *Id.*

[43] Security Architecture, https://www.lastpass.com/security (last accessed March 6, 2023). LastPass has since removed some of the quoted passages from its webpage, but the page as accessed by Plaintiffs' counsel can be seen in its original form via The Wayback Machine. https://web.archive.org/web/20230131095549/https://www.lastpass.com/security.

[44] *Id.*

273. Not all of LastPass's security claims appear to be accurate. For instance, LastPass only requires 100,100 iterations of the PBKDF2 algorithm[45] to secure customers' master passwords, which is well below the standard 310,000 iterations recommendation by the Open Web Application Security Project ("OWASP").[46]

274. Indeed, at the time of the Data Breach, LastPass had failed to update its master password encryption requirements since as early as 2018, a lifetime by cybersecurity standards.[47]

275. LastPass did not incorporate these protective measures into its requirements, despite its claim that "[w]e routinely test the latest password cracking technologies against our algorithms to keep pace with and improve upon our cryptographic controls."[48]

276. Even LastPass's claims that its password requirements are sufficient is inaccurate. While LastPass leads its customers to believe that a twelve-character minimum for master passwords "greatly minimizes the ability for successful brute force password guessing," and that "it would take millions of years to guess your master password using generally-available password-cracking technology," modern graphics processors can crack human-chosen (as opposed

---

[45] "About Password Iterations, https://support.lastpass.com/help/about-password-iterations-lp030027 (last accessed on Jan. 13, 2023). As of January 13, 2023, LastPass used the PBKDF2 algorithm to change a customer's master password into a login hash string which is communicated to LastPass to authenticate the customer as the correct user. Since the filing of various complaints consolidated in this action, LastPass has since updated its requirement to 600,000 iterations. LastPass's January recommendations are accessible via the Wayback Machine. https://web.archive.org/web/20230203004335/https://support.lastpass.com/help/about-password-iterations-lp030027.

[46] OWSAP Cheat Sheet Series, Password Storage Cheat Sheet, https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html#pbkdf2 (last accessed Jan. 13, 2023). These recommendations have recently changed to 600,000 iterations for SHA-256 algorithms, which are currently reflected on OWSAP's website.

[47] What's in a PR statement: LastPass breach explained, https://palant.info/2022/12/26/whats-in-a-pr-statement-lastpass-breach-explained/ (last accessed July 14, 2023).

[48] Toubba, Karim, Notice of Recent Security Incident, https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/ (posted December 22, 2022).

to truly random), PBKDF2-protected passwords "in slightly more than two months" using just a single processor, and those speeds are only getting faster.[49] This is particularly troubling considering that while LastPass requires new customers to use a twelve-character master password to secure their password vault, when that change was made in 2018, the company did not require, and has not since required, that current customers update their shorter, less-secure master passwords to a twelve-character minimum.[50]

277. Despite claiming many features designed to protect customer password vaults from direct attacks, which appear to have been haphazardly employed at best, LastPass also did not manage its own cybersecurity systems to ensure that copies were not made of customer password vaults, including the password vaults belonging to Plaintiffs and Class Members.

278. In fact, LastPass's lax cybersecurity controls within its own environment allowed a threat actor to enter its development environment in August 2022, using a compromised employee developer account, ultimately allowing the threat actor to obtain credentials and keys to access and decrypt storage volumes within LastPass's cloud-based storage service, and exploit source code and technical information stolen from LastPass's development environment to gain customer account information and related metadata including company names, end-user names, billing addresses, email addresses, telephone numbers, IP addresses from which customers were accessing the LastPass service, and backup copies of LastPass's customer vaults containing data such as website URLs, website usernames, passwords, secure notes, and form-filled data."[51]

---

[49] What's in a PR statement: LastPass breach explained, https://palant.info/2022/12/26/whats-in-a-pr-statement-lastpass-breach-explained/ (posted December 26, 2022).

[50] *Id.*

[51] Toubba, Karim, Notice of Recent Security Incident, https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/ (posted December 22, 2022).

279. Sophisticated companies like LastPass are aware of the types of threat actors across the Internet and the types of security exploits they employ for profit. Accordingly, it is imperative that, as a company specializing in and profiting from providing data security services to others, it guard against those exploits.

280. Particularly prevalent today are iterative attacks, which begin with seemingly innocuous probes of a website by hackers hoping to build knowledge of the infrastructure and to search out potential vulnerabilities, before returning weeks or months later with more powerful tools and better knowledge about the target's defenses. This is the nature of the Data Breach here.

C. GoTo Failed to Require that LastPass Implement Appropriate Internal Cybersecurity Protections

281. GoTo acquired LastPass in October of 2015.[52]

282. Upon information and belief, and based upon standard cybersecurity practices, during that acquisition process, GoTo was informed of the various cybersecurity and data privacy risks present in LastPass's systems.

283. Both prior to its acquisition by GoTo and since, LastPass's inadequate cybersecurity measures were apparent.

284. For instance, on May 3, 2011, LastPass suffered a security incident. GoTo would have known about this incident when it acquired LastPass. LastPass was unable to state for certain that customer information was not breached, requiring some users to change their master passwords as a precaution.[53]

---

[52] *See* Joe Siegrist, LastPass Joins the LogMeIn Family (posted October 9, 2015) (no longer available LastPass' website, but available at The Wayback Machine, https://web.archive.org/web/20160112075212/https://blog.lastpass.com/2015/10/lastpass-joins-logmein.html/, last accessed on July 11, 2023).

[53] *See* JR Raphael, LastPass CEO Explains Possible Hack, PCWorld (May 5, 2011), https://www.pcworld.com/article/491164/lastpass_ceo_exclusive_interview.html.

285. On June 15, 2015, LastPass posted on a blog that it had suffered a data breach.[54] The LastPass investigation revealed that LastPass account email addresses, password reminders, server per user salts, and authentication hashes were compromised.

286. In July 2016, a vulnerability was discovered by independent online security firm Detectify. Detectify published a blog post on the vulnerability, describing it as a bug in the autofill function that allowed for the extraction of passwords.[55]

287. In March 2017, a vulnerability was discovered in the LastPass browser extension for Chrome that applied to all LastPass clients.[56]

288. In August 2019, a vulnerability in the LastPass browser extension for Chrome and Opera browsers allowed malicious websites to steal credentials for the last account the user logged into.[57]

289. In 2020, a vulnerability in the LastPass browser extension was revealed, where the extension would store a user's master password in a local file when the "Remember password" option was activated.[58]

---

[54] *See* Joe Siegrist, LastPass Hacked—Identified Early & Resolved, Update as of June 15, 2015, https://blog.lastpass.com/2015/06/lastpass-security-notice/.

[55] *See* Mathias Karlsson, How I made LastPass give me all your passwords, Detectify (Jul. 27, 2016), https://labs.detectify.com/2016/07/27/how-i-made-lastpass-give-me-all-your-passwords/.

[56] Travis Ormandy (@taviso), Twitter (Mar. 25, 2017), https://twitter.com/taviso/status/845717082717114368.

57 Dan Goodin, Password-exposing bug purged from LastPass extensions, Ars Technica (Sept. 16, 2019), https://arstechnica.com/information-technology/2019/09/lastpass-fixes-bug-that-leaked-the-password-of-last-logged-in-account/.

[58] *See* Oleg Afonin, Breaking LastPass: Instant Unlock of the Password Vault (Apr. 6, 2020), https://blog.elcomsoft.com/2020/04/breaking-lastpass-instant-unlock-of-the-password-vault/.

290. In 2021, it was discovered that the LastPass Android app contained seven third-party trackers that sent data to third-party companies and recorded user behavior.[59]

291. In December 2021, users reported that their LastPass master passwords appeared to be compromised. LastPass responded to the news, noting that they had been investigating reports of users receiving e-mails alerting them to block login attempts.[60]

292. Despite this extensive history of cybersecurity incidents, GoTo did not require LastPass to implement sufficient cybersecurity standards and practices, either internally for its own employees and systems, or for its customers.

293. Despite being its parent company, and in a position to do so, GoTo did not direct LastPass to secure its systems using up-to-date cybersecurity protections that would have substantially reduced the damage done by the Data Breach, if not preventing it entirely.

294. GoTo was still LastPass's parent company when LastPass assured its customers in an initial notice on August 25, 2022, that there was "no evidence that this incident involved any access to customer data or encrypted password vaults"[61] and that the "LastPass security team had "contained the incident." [62] This was not only untrue, it was only the beginning.

D. Security Failures Result in the Exposure of Customer Data

295. At some point before August 2022 (it is unclear exactly when, as LastPass has refused to provide this information) a threat actor was able to achieve persistent entry to LastPass's

---

[59] *See* Jon Porter, Security researcher recommends against LastPass after detailing 7 trackers, The Verge (Feb. 26, 2021), https://www.theverge.com/2021/2/26/22302709/lastpass-android-app-trackers-security-research-privacy.

[60] *See* Emma Roth, LastPass says no passwords were compromised following breach scare, The Verge (Dec. 28, 2021), https://www.theverge.com/2021/12/28/22857485/lastpass-compromised-breach-scare.

[61] *Id.*

[62] *Id.*

back-end, developer environments, and cloud-based servers. This same threat actor was also able to extract LastPass customer logins and passwords (or "credentials.") By obtaining customers' credentials, the threat actor was obtaining access to backups of each customer's vault, even if the vault (as LastPass claims) was encrypted. Unfortunately, LastPass's much-vaunted ""Zero-Knowledge Encryption Model" did not prevent hackers from getting access to their customers' most valuable PII, and credentials for dozens (if not hundreds) of other websites.

296. Despite this, LastPass assured its customers in its August 25, 2022 notification of the Data Breach that it had "deployed containment and mitigation measures, and engaged a leading cybersecurity and forensics firm" and that it had "achieved a state of containment, implemented additional enhanced security measures, and [saw] no further evidence of unauthorized activity."[63]

297. In that same notice, LastPass explicitly averred that customers' "Master Passwords"—the master key to unlock vaults containing hidden passwords to customers' online accounts and PII—remained uncompromised.[64] LastPass further claimed that no data within customers' vaults and no personal information had been compromised, and that the corporation's security measures continued to "ensure[] that only the customer has access to decrypt vault data."[65]

298. LastPass was so dismissive of the serious impacts of the Data Breach that, in response to the frequently asked question, "What should I do to protect myself and my vault data?", LastPass answered: "At this time, we don't recommend any action on behalf of our users or administrators."[66] Customers who sought more information beyond the blog post were met with

---

[63] Toubba, Karim, Notice of Recent Security Incident (posted August 25, 2022) https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/.

[64] *Id.*

[65] *Id.*

[66] *Id.*

the statement that LastPass would "continue to update [its] customers with the transparency they deserve."[67]

299. On September 15, 2022, a month after the Data Breach began, LastPass released a second blog post to "update" its customers, including Plaintiffs and Class Members, on the "conclusion" of its investigation and "to provide transparency and peace-of-mind to our consumer and business communities."[68]

300. LastPass again confirmed there was no evidence that the Data Breach involved access to customer data or password vaults. LastPass made this assurance despite admitting that its investigations into the mechanics of the initial Data Breach were "inconclusive" and that the cyber attacker had "persistent access" such that they could "impersonate" a LastPass employee-developer and thereby access the development environment.[69] The admission that the threat actor had managed to "impersonate" a LastPass employee-developer masked a more frightening truth: for the first time, LastPass revealed that the threat actor had managed to defeat LastPass's multifactor authentication measures.[70]

301. Instead of saying this outright, LastPass explicitly assured customers that their "data and passwords are safe in our care," and described the company's investigation into the Data Breach as "completed."[71]

---

[67] *Id*.

[68] *Id.*

[69] *Id*.

[70] *Id.* ("the threat actor utilized their persistent access to impersonate the developer once the developer had successfully authenticated using multi-factor authentication.").

[71] *Id*.

302. The Data Breach, despite LastPass's assurances that it "was limited to a four-day period in August 2022," was actually a deliberate, methodical, and continuing invasion of LastPass's security systems, culminating in the copying of customer password vaults, including the password vaults belonging to Plaintiffs and Class Members.

303. Along with assurances that LastPass had "partnered with a leading cyber security firm to further enhance our existing source code safety practices" and "deployed enhanced security controls including additional endpoint security controls and monitoring," LastPass made this fateful promise: "We recognize that security incidents of any sort are unsettling but want to assure you that your personal data and passwords are safe in our care."[72]

304. For two and a half months, LastPass gave its customers assurance that their data and passwords were safe in the care of LastPass, until, on November 30, 2022, LastPass posted an update to its security incident blog, informing its customers, including Plaintiffs and Class Members, that it had "detected unusual activity within a third-party cloud storage service" shared by LastPass and its affiliate, GoTo. LastPass also admitted, for the first time, that the "unauthorized party, using information obtained in the August 2022 incident, was able to gain access to certain elements of our customers' information."[73]

305. For the first time, LastPass admitted that it did not at the time know "the scope of the incident" or "what specific information has been accessed," and indicated that it was continuing to "deploy enhanced security measures and monitoring capabilities across our infrastructure to help detect and prevent further threat actor activity."[74]

---

[72] *Id.*

[73] *Id.*

[74] *Id.*

306. For the first time, LastPass also revealed that the initial August breach had spread to LastPass's third-party cloud storage service—shared by both LastPass and GoTo—and that it was the information and data obtained in the August breach that allowed threat actors to expand their reach in November 2022.

307. Even after discovering this expanded breach activity, LastPass failed to provide its customers with any specific recommendations about security measures they could take, beyond pointing to LastPass's password best practices. [75]

308. Again, LastPass provided false hope, stating that "customers' passwords remain safely encrypted." [76]

309. Finally, on December 22, 2022, more than four months after the Data Breach began, LastPass CEO Karim Toubba revealed that the threat actor had not only "gained access to a third-party cloud-based storage service" but had also obtained the company's "cloud storage access key and dual storage container decryption keys."[77] LastPass admitted that using these keys obtained in the Data Breach, the threat actor copied customer PII "from backup."[78]

310. As a result of the Data Breach, LastPass admitted the exposure of "customer account information and related metadata including company names, end-user names, billing addresses, email addresses, telephone numbers, and the IP addresses from which customers were accessing the LastPass service." [79] LastPass explained that "[t]he threat actor was also able to copy a backup of customer vault data from the encrypted storage container which is stored in a

---

[75] *Id.*

[76] *Id.*

[77] *Id.*

[78] *Id.*

[79] *Id.*

proprietary binary format that contains both unencrypted data, such as website URLs, as well as fully-encrypted sensitive fields such as website usernames and passwords, secure notes, and form-filled data."[80]

311. In addition, although LastPass maintains that user passwords were encrypted, it nevertheless acknowledged that "[t]he threat actor may attempt to use brute force to guess your master password and decrypt the copies of vault data they took."[81] This is a serious acknowledgement. LastPass is thus *effectively* admitting that the threat actor now had a limitless amount of time to crack the passwords on users' password vaults, and LastPass customers, including Plaintiffs and Class Members, had no way of resetting their passwords to prevent this from occurring.[82]

312. After this revelation, LastPass informed its customers that it had "eradicated any further potential access to the LastPass development environment by decommissioning that environment in its entirety and rebuilding a new environment from scratch," "replaced and further hardened developer machines, processes, and authentication mechanisms," "added additional logging and alerting capabilities to help detect any further unauthorized activity including a second line of defense with a leading managed endpoint detection and response vendor to supplement our own team," and began "actively rotating all relevant credentials and certificates that may have

---

[80] *Id.*

[81] *Id.*

[82] One publication pointed out that the theft of backups "pose[s] a particular problem for users seeking to protect themselves in the wake of the breach, because changing that primary password now with LastPass won't do anything to protect the vault data that's already been stolen." *Yes, It's Time to Ditch LastPass,* Lily Hay Newman, Wired, Dec. 28, 2022 (available at https://www.wired.com/story/lastpass-breach-vaults-password-managers/).

been affected and supplementing existing endpoint security."[83] LastPass did not explain why such additional security measures were not implemented in August 2022, or why they were not in place already, to better secure its environments against threat actors intent on causing harm and stealing its customers PII.

313. LastPass also stated that it was "performing an exhaustive analysis of every account with signs of any suspicious activity within our cloud storage service, adding additional safeguards within this environment, and analyzing all data within this environment to ensure we understand what the threat actor accessed."[84] Again, LastPass did not offer an explanation as to why these security protections were not in place in advance of the Data Breach, or at the very least, employed as soon as LastPass became aware of the intrusion in August 2022.

314. LastPass also finally offered, after four months, its first *prospective* recommendation to its users on how to protect themselves, advising that users "should consider minimizing risk by changing passwords of websites you have stored."[85] Less helpfully, it again provided a "password settings and best practices" guide that predated the Data Breach and could not possibly help Plaintiffs and Class Members prevent theft of their already stolen information.

315. Incredibly, LastPass also admitted that the company had, as of its December 2022 notice, notified less than 3% of its business customers to recommend that they take any action at all.[86]

---

[83] Toubba, Karim, Notice of Recent Security Incident (Dec. 22, 2022), https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/.

[84] *Id.*

[85] *Id.*

86 *Id.*

316. Three months later, in March of 2023, LastPass posted an update regarding their "exhaustive" investigation and purporting to explain to its customers how the Data Breach occurred, and what its customers can do now.[87] Placeholder.

317. LastPass stated that it spent "a significant amount of time and effort hardening [its] security while improving overall security operations" in its March update, but did not explain why those protections were not already in place, particularly considering the premium its customers place on the security of their data.[88]

318. LastPass again attempted to shift blame, pointing at "a vulnerability in third-party software" as the reason the threat actor was able to gain access to its systems, eliding past the fact that the third-party software was deployed by its own employee, and that the initial intrusion went undetected for weeks, if not months.[89]

319. In March, LastPass for the first time acknowledged that the "data accessed [by the threat actor] from those backups included system configuration data, API secrets, third-party integration secrets, and *encrypted and unencrypted LastPass customer data*."[90]

320. Among the customer data accessed by the threat actor, LastPass identified "customer metadata, and backups of all customer vault data."[91]

---

[87] Toubba, Karim, Security Incident Update and Recommended Actions (Mar. 1, 2023), https://blog.lastpass.com/2023/03/security-incident-update-recommended-actions/.

[88] *Id.*

[89] *Id.*

[90] *Id.*

[91] *Id.*

321. Despite these revelations, LastPass continued to offer only *prospective* advice on how to avoid *future* account intrusions for personal[92] and business[93] accounts.

322. Perhaps most incongruously, LastPass's CEO Karim Toubba stated that he had spoken with many customers, and understood their frustration not at the size or extent of the Data Breach itself, but at the "inability to communicate more immediately, more clearly, and more comprehensively throughout this event."[94]

323. Mr. Toubba stated in his post that he did "accept the criticism and take full responsibility."[95]

324. Mr. Toubba, and his company, clearly do not understand the nature of the grievances expressed to them: LastPass advertised internet security, and none of its customers got what was advertised. Now, instead of the stable internet security regime that they signed up for, LastPass's customers are left wondering what information of theirs was exposed, and how that exposure might contribute to a future harm, if one has not already befallen them.

E. Data Breaches Put Consumers at Increased Risk of Fraud and Identify Theft

325. PII is valuable property. Its value is axiomatic, considering the market value and profitability of "Big Data" to corporations in America. Illustratively, Alphabet Inc., the parent

---

92 Security Bulletin: Recommended Actions for Free, Premium, and Families Customers, https://support.lastpass.com/s/document-item?language=en_US&bundleId=lastpass&topicId=LastPass/security-bulletin-recommended-actions-free-premium-families.html&_LANG=enus (last accessed July 17, 2023).

93 Security Bulletin: Recommended Actions for LastPass Business Administrators, https://support.lastpass.com/s/document-item?language=en_US&bundleId=lastpass&topicId=LastPass/security-bulletin-recommended-actions-business-administrator.html&_LANG=enus (last accessed July 17, 2023).

94 Toubba, Karim, Security Incident Update and Recommended Actions (Mar. 1, 2023), https://blog.lastpass.com/2023/03/security-incident-update-recommended-actions/.

95 *Id.*

company of Google, reported in its 2020 Annual Report a total annual revenue of $182.5 billion and net income of $40.2 billion.[96] $160.7 billion of this revenue derived from its Google business, which is driven almost exclusively by leveraging the PII it collects about the users of its various free products and services.

326. Criminal law also recognizes the value of PII and the serious nature of the theft of PII by imposing prison sentences. This strong deterrence is necessary because cybercriminals extract substantial revenue through the theft and sale of PII. Once a cybercriminal has unlawfully acquired PII, the criminal can demand a ransom or blackmail payment for its destruction, use the PII to commit fraud or identity theft, or sell the PII to other cybercriminals on the black market.

327. Cybercriminals use "ransomware" to make money and harm victims. Ransomware is a widely known and foreseeable malware threat in which a cybercriminal encrypts a victim's computer such that the computer's owner can no longer access any files or use the computer in any way. The cybercriminal then demands a payment for the decryption key. Ransomware is typically propagated through phishing, spear phishing, or visiting a malicious or compromised website that contains a virus or other malware.

328. Once stolen, PII can be used in many ways. PII can be offered for sale on the "dark web," a heavily encrypted part of the Internet that makes it difficult for authorities to detect the location or owners of a website. The dark web is not indexed by normal search engines such as Google and is only accessible using a Tor browser (or similar tool), which aims to conceal users' identities and online activity. The dark web is notorious for hosting marketplaces selling illegal

[96] Alphabet Inc., Annual Report (Form 10-K) at 32 (Feb. 3, 2021), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001652044/000165204421000010/goog-20201231.htm.

items such as weapons, drugs, and PII. Websites appear and disappear quickly, making it a dynamic environment.

329. The U.S. government, various U.S. and international law enforcement agencies, cybersecurity industry groups and laboratories, and numerous industry trade groups have issued warnings and guidance on managing and mitigating phishing and ransomware threats. There are industry best practices for cybersecurity related to phishing and ransomware, some of which are particularly effective.

330. For example, in 2019, both Microsoft and Google publicly reported that using multi-factor authentication ("MFA") blocks more than 99% of automated hacks, including most ransomware attacks that occur because of unauthorized account access. Likewise, the reputable SANS Software Security Institute issued a paper stating "[t]ime to implement multi-factor authentication!"[97] An example of MFA implementation is receiving a text with a code when you input your username and password into a website; even if a cybercriminal knew your username and password, the cybercriminal would not be able to see the code on your phone and would thus be blocked from accessing your online account.

331. In this regard, implementing MFA "can block over 99.9 percent of account compromise attacks."[98]

332. The FBI concurs, listing "applying two-factor authentication wherever possible" as a best practice to defend against ransomware attacks.[99]

---

[97] Matt Bromiley, Bye Passwords: New Ways to Authenticate at 3, SANS Software Security Inst. (July 2019), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3y9UJ.

[98] What Is Multi-Factor Authentication (MFA)?, Consensus Techs. (Sept. 16, 2020), https://www.concensus.com/what-is-multi-factor-authentication.

[99] Ransomware Victims Urged to Report Infections to Federal Law Enforcement, FBI (Sept. 15, 2016), https://www.ic3.gov/Media/Y2016/PSA160915.

333. The industries that LastPass serves have seen a substantial increase in cyberattacks and data breaches since as early as 2016.[100]

334. Indeed, cyberattacks have become so notorious that the FBI and Secret Service issued a warning in 2019 to potential targets so they were aware of, and prepared for, a potential attack.[101]

335. The GAO explains that "[t]he term 'identity theft' is broad and encompasses many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit card account in someone else's name."[102] The GAO Report notes that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[103]

336. The Federal Trade Commission ("FTC") recommends that identity theft victims take several steps to protect their personal health and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and to consider an extended fraud alert that lasts for seven years if identity theft occurs), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[104]

---

[100] *Id.*

[101] Kochman, *supra* n.171.

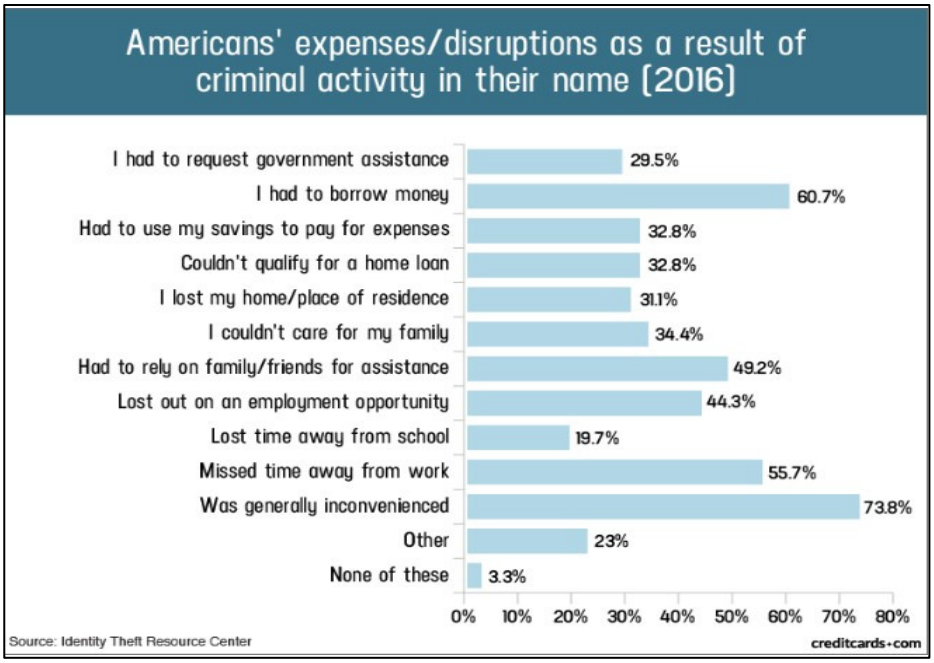
[102] U.S. Gov't Accountability Office, GAO–07–737, Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown 2 (2007), *available at* gao.gov/assets/gao-07-737.pdf.

[103] *Id.*

[104] Identity Theft Recovery Steps, FTC, https://www.identitytheft.gov/Steps (last accessed Mar. 23, 2021). Indeed, the FTC takes data breaches seriously, and has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal

337. Cybercriminals use stolen PII such as social security numbers ("SSNs") for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

338. Identity thieves can also use SSNs to obtain a driver's license or other official identification card in the victim's name, but with the thief's picture; use the victim's name and SSN to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house or receive medical services in the victim's name, seek unemployment or other benefits, and may even give the victim's PII to police during an arrest resulting in an arrest warrant being issued in the victim's name. A study by the Identity Theft Resource Center ("ITRC") shows the multitude of harms caused by fraudulent use of personal and financial information:



105

information can constitute an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

[105] Jason Steele, Credit Card and ID Theft Statistics, Creditcards.com (updated Oct. 24, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.

339. As set forth above, 96.7% of study subjects experienced costs or other harms from the criminal activity.[106] As illustrated in the above graphic, this includes devastating results such as "I lost my home/place of residence" and "I couldn't care for my family." Moreover, the harms of identity theft are not limited to the affected individual and may adversely impact other associated persons and support systems, including government assistance programs. In the ITRC study, nearly one third of survey respondents had to request government assistance because of identity theft, such as welfare, EBT, food stamps, or similar support systems.[107] The ITRC study concludes that "identity theft victimization has an extreme and adverse effect on each individual as well as all of the support systems and people associated with the individual."[108]

340. PII is a valuable property right.[109] Its value is axiomatic, considering the value of Big Data in corporate America as well as the consequences of cyber thefts resulting in heavy prison sentences. This obvious risk to reward analysis illustrates that Private Information has considerable market value that is diminished when it is compromised.

341. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when PII and/or financial information is stolen and when it is used. According to the GAO, which conducted a study regarding data breaches: "[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once

---

[106] *Id.*

[107] *Id.*

[108] *Id.*

[109] *See, e.g.*, John T. Soma et al., Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *1 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.").

stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[110]

342. PII is such an inherently valuable commodity to identity thieves that, once it is compromised, criminals often trade the information on the cyber black-market for years.

343. Furthermore, data breaches that expose any personal data, and in particular non-public data of any kind (e.g., donation history or hospital records), directly and materially increase the chance that a potential victim is targeted by a spear phishing attack in the future, and spear phishing results in a high rate of identity theft, fraud, and extortion.[111]

344. There is a strong probability that much of the information stolen in the Data Breach has not yet been made available on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. Indeed, some of the Class Members are in very early stages of their lives—in their twenties and thirties. Thus, as the respective Notices advise, customers, including Plaintiffs and Class Members, must vigilantly monitor their financial accounts for many years to come.

345. This problem will only get worse: a study published in May 2022 by the International Data Corporation projects that the amount of new data created, captured, replicated,

---

[110] GAO Report, *supra* at 29.

[111] *See* Kelion & Tidy, *supra* (concluding that personal information such as "names, titles, telephone numbers, email addresses, mailing addresses, dates of birth, and, more importantly, donor information such as donation dates, donation amounts, giving capacity, philanthropic interests, and other donor profile information .....in the hands of fraudsters, [makes consumers] particularly susceptible to spear phishing—a fraudulent email to specific targets while purporting to be a trusted sender, with the aim of convincing victims to hand over information or money or infecting devices with malware").

and consumed is expected to double in size by 2026.[112] With an increase in data creation comes a heightened risk of data breaches and bad actors gaining access to personal information. One result of data breaches, identity theft, poses a serious threat to consumers engaging in online transactions and across a host of digital platforms. Both state and federal laws and regulations impose standards of reasonable security measures for businesses so consumers can, in turn, feel safe sharing their PII in the marketplace.

346. Data privacy is important to the public: according to a survey conducted by cyber-security company FireEye, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[113]

347. Data breaches are not an unpreventable occurrence. In the Data Breach and Encryption Handbook, Lucy Thompson wrote, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions." She continued, "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised "[114]

---

[112] *See* John Rydning, Worldwide IDC Global DataSphere Forecast, 2022–2026: Enterprise Organizations Driving Most of the Data Growth, IDC, *available at* https://www.idc.com/getdoc.jsp?containerId=US49018922 (last accessed Jan. 18, 2023).

[113] FireEye, Beyond the Bottom Line: The Real Cost of Data Breaches (May 11, 2016), https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last accessed March 5, 2021).

[114] Lucy L. Thomson, Data Breach and Encryption Handbook (Am. Bar Assoc. 2011).

348. The theft of Plaintiffs' and Class Members' personal information is all the more galling considering that they took specific steps to protect it: by the very virtue of using the service provided by LastPass (many for a subscription fee), Plaintiffs showed that they care deeply about data privacy and security. Now, due to the Defendant's failures, Plaintiffs have entirely lost the benefit of that bargain.

349. Cyber criminals can use the financial information that Defendants were entrusted to safeguard to perpetrate financial crimes that harm Plaintiffs and the Class, or as what appears to have happened to Defendants in this instance, cyber criminals can leverage pieces of information to gain access to additional information that they can then use to carry out significant financial harm to victims. In addition to all the other immediate consequences of the LastPass Data Breach, Plaintiffs and Class Members face a substantially increased risk of identity theft.

F. LastPass Failed to Inform Customers of the True Extent of the Data Breach, and Has Not Yet Done So

350. LastPass has made a show of continuing to provide "transparency"[115] in its Data Breach updates but has failed to provide a complete and accurate picture of the risks currently facing LastPass customers, including Plaintiffs and Class Members.

351. To begin with, LastPass only recently informed its customers that more than one intrusion was made into its system, and that the Data Breach first detected in August 2022 was more damaging than previously acknowledged. On December 22, 2022, LastPass posted in a notice on its website that "we have learned that an unknown threat actor accessed a cloud-based

[115] Toubba, Karim, Notice of Recent Security Incident (Dec. 22, 2022) https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/.

storage environment leveraging information obtained from the incident we previously disclosed in August of 2022."[116]

352. Only in December did LastPass disclose that the source code and technical information stolen in the August intrusion was used to target a LastPass employee, through which the threat actor obtained customer credentials and keys used to access and decrypt storage volumes within the cloud-based storage service.[117]

353. Only then did they disclose that cloud storage access keys and dual storage container decryption keys were obtained by the threat actor, and that the threat actor copied information from backups that contained basic customer account information and related metadata including company names, end-user names, billing addresses, email addresses, telephone numbers, and the IP addresses from which customers, including Plaintiffs and Class Members, were accessing the LastPass service, before extracting that information.[118]

354. Since August 22, 2022, the beginning of the Data Breach, LastPass has yet to announce a single actionable recommendation. LastPass has continually referred to its "password best practices,"[119] which it claims will prevent hackers from using "brute force to guess [the] master password and decrypt the copies of vault data they took."[120]

355. LastPass continues to assert that customer master passwords were not exposed in the Data Breach, but this is belied by Plaintiffs' own experiences. [redacted]

---

[116] *Id.*

[117] *Id.*

[118] *Id.*

[119] What is the LastPass Master Password?, https://support.lastpass.com/help/what-is-the-lastpass-master-password-lp070014.

[120] Toubba, Karim, Notice of Recent Security Incident (Dec. 22, 2022), https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/.

[redacted]

356. This leaves only two possibilities: LastPass has not been honest about the extent of the Data Breach, and have not disclosed that its customers' LastPass login credentials were compromised, or (perhaps even worse), LastPass *has not yet figured this out.*

357. Even if it were true that customer master passwords were not implicated in the Data Breach, LastPass has given its customers no conception of how long their vaults have been in the hands of threat actors: a particularly important data point when determining whether customers' vaults might be vulnerable to brute force attacks.

358. Instead, LastPass offers platitudes: "it would be extremely difficult to attempt to brute force guess master passwords."[122]

359. The copying of password vaults, combined with the time from when the initial intrusion occurred and when LastPass announced the Data Breach, have given cybercriminals months to break into those vaults and compromise the login credentials held there. Such lack of notice has made it much more likely that Plaintiffs and Class Members will suffer irreparable harm, including the loss of control over their accounts, including passwords and PII.

360. Despite the desperate need for additional information, to permit LastPass customers, including Plaintiffs and Class Members, to assess the extent of the danger to their accounts, including their PII, and to take appropriate protective steps, LastPass has merely offered advice for protection of accounts that would be effective only prior to the Data Breach, and thinly-disguised, rehabilitative marketing.

---

[121] *Id.*

[122] *Id.*

361. Indeed, all of LastPass's suggestions are self-serving attempts to shift liability to its customers, including Plaintiffs and Class Members, if their password is cracked by brute force. In its December post, under the heading "What Should LastPass Customers Do?", LastPass states only the following:[123]

- Since 2018, we have required a twelve-character minimum for master passwords. This greatly minimizes the ability for successful brute force password guessing.
- To further increase the security of your master password, LastPass utilizes a stronger-than-typical implementation of 100,100 iterations of the Password-Based Key Derivation Function (PBKDF2), a password-strengthening algorithm that makes it difficult to guess your master password. You can check the current number of PBKDF2 iterations for your LastPass account here.
- We also recommend that you never reuse your master password on other websites. If you reuse your master password and that password was ever compromised, a threat actor may use dumps of compromised credentials that are already available on the Internet to attempt to access your account (this is referred to as a "credential stuffing" attack).

362. None of the advice provided by LastPass recommends future actions, which is worthless, because the proverbial horse has already left the barn. Judging by LastPass's own press releases, the intrusion into its systems (in December of 2022) was at least five months old, and LastPass has no meaningful recommendations for how its customers might avoid phishing scams, cracking of their password vaults, or any other identity theft or fraud.

363. Instead of steps Plaintiffs and Class Members could take to protect themselves from a future hack, credential-stuffing, or phishing activity, such as changing individual site passwords, obtaining credit and dark web monitoring, and freezing their credit, LastPass told its customers,

[123] *Id.*

including Plaintiffs and Class Members: "There are no recommended actions that you need to take at this time."[124]

364. LastPass does explain that if a customer's "master password does not make use of the defaults above, then it would significantly reduce the number of attempts needed to guess it correctly" and advises that, if this is the case, customers should "consider minimizing risk by changing passwords of websites" they have stored.[125] However, LastPass has not contacted its customers, including Plaintiffs and Class Members, to inform them if their passwords do not meet LastPass's minimum thresholds, even if those minimum thresholds themselves are potentially insufficient, considering the development of brute-forcing technology and the growth in technical prowess of hackers and cybercriminals.

365. LastPass's notifications of the Data Breach have failed to provide sufficient information or recommendations to its customers, including Plaintiffs and Class Members, and have attempted to shift blame for any compromise of PII to its customers, including Plaintiffs and Class Members.

366. As a result of LastPass's deficient notifications, Plaintiffs and Class Members do not have an understanding of the risks currently facing them. These risks are real and imminent, and LastPass is under a duty to provide information to its customers, including Plaintiffs and Class Members, to permit them to protect themselves from further compromise. LastPass has either failed, or refused, to do this.

367. As a result of the Data Breach, and LastPass's refusal to provide consumers, including Plaintiffs and Class Members, with basic information needed to protect themselves and

---

[124] *Id.*

[125] *Id.*

take specific, preventative measures, customers, including Plaintiffs and Class Members, incurred, and will continue to incur, out-of-pocket costs. Such out-of-pocket costs include identity theft protection and insurance services, as well as time spent taking preventative measures and responding to identity theft and fraud.

G. Defendants Caused Plaintiffs and Class Members Actual, Concrete, and Preventable Harm

368. As a result of the Data Breach, Plaintiffs and millions of Class Members have suffered and will continue to suffer concrete and actual harm. LastPass promised to safeguard Plaintiffs' and Class Members' sensitive PII, including passwords securing highly sensitive accounts. As a result of the Data Breach, Plaintiffs' and Class Members' sensitive PII was compromised, unlawfully accessed, and made subject to unlawful use by cybercriminals.

369. Despite these promises, Plaintiffs' and Class Members' sensitive PII—including passwords securing their most sensitive accounts, which were entrusted to LastPass—was compromised, unlawfully accessed, and made subject to unlawful use by cybercriminals, as a result of the Data Breach.

370. In addition to initially failing to deliver on its promise to maintain Plaintiffs' and Class Members' PII safely and securely prior to the Data Breach—by, for example, ensuring proper company security protocols were in place and ensuring customers followed security best practices—LastPass's gross mismanagement made a bad breach worse.

371. LastPass failed to give adequate notice to customers about the extent and severity of the Data Breach in real time (or even near real time). In a wide-ranging Data Breach that spanned nearly five months, LastPass provided four communications to customers, only two of which made clear that customer data was exposed. As a result, Plaintiffs and Class Members were left in the dark about whether and to what extent sensitive PII was exposed. Further, Plaintiffs and Class

Members were unable to make informed decisions about seeking to mitigate harm resulting from the Data Breach, such as by procuring credit reporting services to assist in the detection of fraud or purchasing password management services from other companies.

372. LastPass was keenly, perhaps uniquely, aware of the risks of cyberattacks and data breaches of its customers' confidential data, including PII. LastPass knew of the risk because it was in the business of helping its customers, including Plaintiffs and Class Members, secure their accounts from hacking, phishing, and other infiltration attempts—indeed, that is LastPass's entire business model. When the Data Breach was initially reported, LastPass stated that it had "deployed containment and mitigation measures," and "achieved a state of containment, implemented additional enhanced security measures, and see no further evidence of unauthorized activity," despite the ongoing threat of further intrusion.[126]

373. It took nearly four months for LastPass to determine that the data stolen and extracted in August 2022 was valuable enough that it would likely subject LastPass to further security intrusions. In November 2022, LastPass announced a further intrusion into its systems which included access to customer data, but LastPass provided only vague statements about the incident, and failed to inform its customers, including Plaintiffs and Class Members, whether or not their data was compromised. Only after LastPass detected yet further intrusions, including extraction of data from its network, did LastPass inform its customers, including Plaintiffs and Class Members, of the potential threats to their most closely protected login credentials and PII.[127]

374. Had LastPass implemented and maintained an appropriate security program, including proper monitoring of its network, security, and communications, LastPass would have

[126] Toubba, Karim, Notice of Recent Security Incident (Aug. 25, 2022), https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/.

[127] *Id.*

discovered the Data Breach sooner or prevented it altogether. In fact, LastPass has announced it has already "eradicated any further potential access to the LastPass development environment by decommissioning that environment in its entirety and rebuilding a new environment from scratch."[128] LastPass also claims to have "replaced and further hardened developer machines, processes, and authentication mechanisms."[129] Had LastPass made these necessary changes previously, the Data Breach would not have happened, and its customers', including Plaintiffs' and Class Members' PII, would not have been accessed, stolen, and now at substantial risk.

375. The Data Breach also exposes Plaintiffs and Class Members to longer-term threats, including identity theft. For victims of a data breach, the risk of identity theft more than quadruples.[130] A data breach can have grave consequences for victims for many years after the breach—with the obtained information, including PII, identity thieves can wreak many forms of havoc: opening new financial accounts, taking out loans, obtaining medical services, obtaining government benefits, or obtaining driver's licenses in the victims' names, forcing victims to guard against potential misuse of their information, including PII.

376. Consumers were denied the benefit of the bargain they struck with LastPass, and instead had their most personal, sensitive information exposed in the Data Breach. Making it even worse, not only was their information exposed, but also the password vaults containing credentials to hundreds of other websites, including email accounts, social media accounts, financial accounts, retirement accounts, and much more.

---

[128] Toubba, Karim, Security Incident Update and Recommended Actions (Mar. 1, 2023), https://blog.lastpass.com/2023/03/security-incident-update-recommended-actions/.

[129] *Id.*

[130] Dave Maxfield & Bill Latham, Data Breaches: Perspectives from Both Sides of the Wall, 25 S.C. Law 28, 30 (May 2014).

377. Plaintiffs and Class Members have already suffered, among other things, actual identity theft, fraud, attempted fraud, significant upticks in phishing, spam, and credential-stuffing attacks, and the additional stress and anxiety of knowing that their personal information was exposed in the Data Breach. In addition, every single LastPass user impacted by the Data Breach is now at an increased risk of future identity theft, cybersecurity attacks, and fraud.

378. As a result of the Data Breach, Plaintiffs and Class Members have suffered concrete damages and harm and are now exposed to a heightened and imminent risk of fraud, identity theft, and targeted phishing attacks for years to come. Furthermore, Plaintiffs and Class Members must now and in the future closely monitor all accounts with information stored using LastPass, spend substantial time resetting passwords associated with each of those accounts, and monitor their financial accounts to guard against identity theft at their own expense. Consequently, Plaintiffs and Class Members have incurred and will continue to incur out-of-pocket costs, including the cost of credit monitoring services, credit freezes, credit reports, and other protective measures, to deter and detect identity theft, among other expenses.

379. By this Complaint, Plaintiffs and Class Members seek to remedy these harms on behalf of themselves and all similarly situated entities, both individual and corporate victims, whose PII was compromised, disclosed, and put at risk, as a result of the Data Breach. Accordingly, Plaintiffs and Class Members bring this action against LastPass seeking redress for its unlawful conduct and assert claims for both common law and statutory damages.

VI. CLASS ACTION ALLEGATIONS

380. Plaintiffs bring this action on their own behalf and on behalf of all natural persons and corporations similarly situated, as referred to throughout this Complaint as "Class Members."

381. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs propose the following Nationwide Class definitions, subject to amendment as appropriate:

> **Nationwide Consumer Class**: All natural persons residing in the United States whose LastPass accounts were compromised, extracted, copied, stolen, or otherwise exposed as a result of the Data Breach.
>
> **Nationwide Business Class:** All companies, entities, and organizations registered to do business in the United States whose LastPass accounts were compromised, extracted, copied, stolen, or otherwise exposed as a result of the Data Breach.

382. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs propose the following Nationwide Subclasses:

> **Nationwide Consumer Contract Subclass:** All Nationwide Consumer Class members who paid for a LastPass account.
>
> **Nationwide Business Class:** All Nationwide Business Class members who paid for a LastPass account.

383. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs propose the following State Subclass definitions, subject to amendment as appropriate:

> **Arizona Consumer Subclass:** All natural persons residing in Arizona whose LastPass accounts were compromised, extracted, copied, stolen, or otherwise exposed as a result of the Data Breach.
>
> **California Consumer Subclass:** All natural persons residing in California whose LastPass accounts were compromised, extracted, copied, stolen, or otherwise exposed as a result of the Data Breach.
>
> **Florida Consumer Subclass:** All natural persons residing in Florida whose LastPass accounts were compromised, extracted, copied, stolen, or otherwise exposed as a result of the Data Breach.
>
> **Illinois Consumer Subclass:** All natural persons residing in Illinois whose LastPass accounts were compromised, extracted, copied, stolen, or otherwise exposed as a result of the Data Breach.
>
> **Massachusetts Consumer Subclass:** All natural persons residing in Massachusetts whose LastPass accounts were compromised, extracted, copied, stolen, or otherwise exposed as a result of the Data Breach.

New York Consumer Subclass: All natural persons residing in New York whose LastPass accounts were compromised, extracted, copied, stolen, or otherwise exposed as a result of the Data Breach.

Oklahoma Consumer Subclass: All natural persons residing in Oklahoma whose LastPass accounts were compromised, extracted, copied, stolen, or otherwise exposed as a result of the Data Breach.

Pennsylvania Consumer Subclass: All natural persons residing in Pennsylvania whose LastPass accounts were compromised, extracted, copied, stolen, or otherwise exposed as a result of the Data Breach.

384. Excluded from the Class and Subclasses are LastPass's officers, directors, and employees; any entity in which LastPass has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of LastPass. Excluded also from the Class and Subclasses are members of the judiciary to whom this case is assigned, their families, and members of their staff.

385. **Numerosity**. The members of the Class (and Subclasses) are so numerous and geographically dispersed that individual joinder of all Class Members is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on LastPass's own statements, the Class consists of more than 33 million individual consumers and at least approximately 100,000 businesses whose accounts were compromised in the Data Breach and can be identified by reviewing the PII exfiltrated from LastPass's databases and by examining LastPass's records.

386. **Commonality**. There are questions of law and fact common to Plaintiffs and Class Members, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether LastPass's data security systems and/or protocol prior to and during the Data Breach complied with applicable data security laws and regulations;

b. Whether LastPass's data security systems and/or protocol prior to and during the Data Breach were consistent with industry standards and best practices;

c. Whether LastPass properly implemented its purported security measures to protect Plaintiffs' and the Class's PII from unauthorized capture, dissemination, and misuse;

d. Whether LastPass took reasonable measures to determine the extent of the Data Breach after it first learned of the same and to timely inform Plaintiffs and the Class as to the nature and extent of the Data Breach, the threat to Plaintiffs and the Class, and the steps Plaintiffs and the Class need to take to protect their information;

e. Whether LastPass disclosed Plaintiffs' and the Class's PII in violation of the understanding that the PII was being stored in confidence and should be maintained;

f. Whether LastPass misrepresented or obfuscated the nature, strength, and extent of its cybersecurity defenses to its account holders;

g. Whether LastPass willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and the Class's PII;

h. Whether LastPass was negligent in failing to properly secure and protect Plaintiffs' and the Class's PII;

i. Whether LastPass was unjustly enriched by its actions; and

j. Whether Plaintiffs and the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

387. **Typicality**. Plaintiffs' claims are typical of those of the Class Members because Plaintiffs' LastPass accounts, like that of every Class Member, were compromised in the Data Breach.

388. **Adequacy of Representation**. Plaintiffs will fairly and adequately represent and protect the interests of Class Members, including those from states and jurisdictions where they do not reside. Counsel representing the Plaintiffs in this action are competent and experienced in

litigating class actions and have been appointed lead counsel by many different courts in many other class action suits.

389. **Predominance**. LastPass has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all Plaintiffs' and Class Members' data at issue here was secured by LastPass and accessed during the Data Breach. The common issues arising from LastPass's conduct affecting Class Members, as described *supra*, predominate over any individualized issues. Adjudication of the common issues in a single action has important and desirable advantages of judicial economy.

390. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for LastPass. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

391. **Injunctive Relief is Appropriate**. LastPass has failed to take actions to safeguard Plaintiffs' and Class Members' PII such that injunctive relief is appropriate and necessary. LastPass has acted on grounds that apply generally to the Class (and Subclasses) as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

VII. CAUSES OF ACTION

CLAIMS ON BEHALF OF THE NATIONWIDE CLASS AND THE SUBCLASSES

FIRST CLAIM FOR RELIEF AND CAUSE OF ACTION
NEGLIGENCE

On Behalf of All Plaintiffs
Against All Defendants

392. Plaintiffs restate and reallege all preceding allegations in paragraphs 1 through 391 as if fully set forth herein.

393. Plaintiffs bring this claim under the law of the Commonwealth of Massachusetts.

394. At all times herein relevant, Defendants owed Plaintiffs and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PII and financial information and to use commercially reasonable methods to do so. Defendants took on this obligation upon accepting and storing the PII and financial information of Plaintiffs and Class Members in its computer systems and on its networks.

395. Among these duties, Defendants were expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII and financial information in its possession;

b. to protect Plaintiffs' and Class Members' PII and financial information using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to quickly detect the Data Breach and to timely act on warnings about data breaches; and

d. to promptly notify Plaintiffs and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII and financial information.

396. Defendants knew that the PII and financial information were private and confidential and should be protected as private and confidential and, thus, Defendants owed a duty

of care not to subject Plaintiffs and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

397. Defendants knew, or should have known, of the risks inherent in collecting and storing PII and financial information, the vulnerabilities of its data security systems, and the importance of adequate security. Defendants knew about numerous, well-publicized data breaches.

398. Defendants knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiffs' and Class Members' PII and financial information.

399. Only Defendants were in the position to ensure that their systems and protocols were sufficient to protect the PII and financial information that Plaintiffs and Class Members had entrusted to them.

400. Defendants breached their duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII and financial information of Plaintiffs and Class Members.

401. Because Defendants knew that a breach of their systems could damage thousands of individuals, including Plaintiffs and Class Members, Defendants had a duty to adequately protect their data systems and the PII and financial information contained therein.

402. Plaintiffs' and Class Members' willingness to entrust Defendants with their PII and financial information was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendants had the ability to protect their systems and the PII and financial information they stored on them from attack. Thus, Defendants had a special relationship with Plaintiffs and Class Members.

403. Defendants also had independent duties under state and federal laws that required Defendants to reasonably safeguard Plaintiffs' and Class Members' PII and financial information

and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendants and Plaintiffs and/or Class Members.

404. Defendants breached their general duty of care to Plaintiffs and Class Members in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII and financial information of Plaintiffs and Class Members;

b. by failing to timely and accurately disclose that Plaintiffs' and Class Members' PII and financial information had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard Plaintiffs and Class Members' PII and financial information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII and financial information;

d. by failing to provide adequate supervision and oversight of the PII and financial information with which it was and is entrusted, despite the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII and financial information of Plaintiffs and Class Members, misuse the PII and intentionally disclose it to others without consent.

e. by failing to adequately train its employees to not store PII and financial information longer than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Plaintiffs' and the Class Members' PII and financial information;

g. by failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and

h. by failing to encrypt Plaintiffs' and Class Members' PII and financial information and monitor user behavior and activity in order to identify possible threats.

405. Defendants' willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

406. As a proximate and foreseeable result of Defendants' grossly negligent conduct, Plaintiffs and Class Members have suffered damages and are at imminent risk of additional harm and damages (as alleged above).

407. The law further imposes an affirmative duty on Defendants to timely disclose the unauthorized access and theft of the PII and financial information to Plaintiffs and Class Members so they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII and financial information.

408. Defendants breached their duty to notify Plaintiffs and Class Members of the unauthorized access by waiting months after learning of the Data Breach to notify Plaintiffs and Class Members and then by failing and continuing to fail to provide Plaintiffs and Class Members sufficient information regarding the breach. To date, Defendants have not provided sufficient information to Plaintiffs and Class Members regarding the extent of the unauthorized access and continues to breach their disclosure obligations to Plaintiffs and Class Members.

409. Further, through their failure to provide timely and clear notification of the Data Breach to Plaintiffs and Class Members, Defendants prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their PII and financial information.

410. There is a close causal connection between Defendants' failure to implement security measures to protect the PII and financial information of Plaintiffs and Class Members and the harm suffered, or risk of imminent harm suffered by Plaintiffs and Class Members. Plaintiffs' and Class Members' PII and financial information were accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII and financial information by adopting, implementing, and maintaining appropriate security measures.

411. Defendants' wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

412. The damages Plaintiffs and Class Members have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendants' grossly negligent conduct.

413. Additionally, 15 U.S.C. §45 (FTC Act, Section 5) prohibits "unfair . . . practices in or affecting commerce," including, as interpreted, and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PII and financial information. The FTC publications and orders described above also form part of the basis of Defendants' duty.

414. Defendants violated 15 U.S.C. §45 by failing to use reasonable measures to protect PII and financial information and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII and financial information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and Class Members.

415. Defendants' violation of 15 U.S.C. §45 constitutes negligence *per se*.

416. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft, (ii) the loss of the opportunity of how their PII and financial information is used, (iii) the compromise, publication, and/or theft of their PII and financial information, (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and financial information, (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to, efforts spent

researching how to prevent, detect, contest, and recover from embarrassment and identity theft, (vi) the continued risk to their PII and financial information, which may remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII and financial information in its continued possession, and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and financial information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

417. As a direct and proximate result of Defendants' negligence and negligence per se, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

418. Additionally, as a direct and proximate result of Defendants' negligence and negligence per se, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their PII and financial information, which remain in Defendants' possession and are subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII and financial information in its continued possession.

419. Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

420. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen its data security systems and monitoring procedures; and (ii) submit to future bi annual audits of those systems and monitoring procedures.

SECOND CLAIM FOR RELIEF AND CAUSE OF ACTION
NEGLIGENT MISREPRESENTATION

On Behalf of All Plaintiffs
Against All Defendants

421. Plaintiffs restate and reallege all preceding allegations in paragraphs 1 through 391 as if fully set forth herein.

422. Plaintiffs bring this claim under the law of the Commonwealth of Massachusetts.

423. Defendants supplied false information for the guidance of others in the course of their business. As alleged in the preceding paragraphs, Defendants falsely represented that their products and services were superior data security practices that would protect Plaintiffs and the Class from the Data Breach, when in reality, Defendants maintained deficient and unreasonable data security practices.

424. Defendants' representations were false, and Defendants failed to exercise reasonable care in obtaining or communicating the information. Defendants' data security measures were unreasonable and deficient by:

a. Failing to conduct proper and reasonable training and due diligence over vendors and employees and data security systems, practices, and procedures;

b. Failing to conduct proper and reasonable due diligence over the employees, vendors or contractors that were the vector(s) of and/or facilitated the hackers' infiltration into the system(s) storing Plaintiffs' and the Class Members' PII;

c. Failing to maintain reasonable and appropriate oversight and audits on their internal data security and their employees, vendors, or contractors that were the vectors of the hackers' infiltration into the system(s) storing Plaintiffs' and the Class Members' PII;

d. Failing to adequately separate and isolate PII from publicly accessible or publicly adjacent environments;

e. Failing to implement and maintain adequate safeguards and procedures to prevent the unauthorized disclosure of Plaintiffs' and the Class members' PII;

f. Failing to monitor and detect their confidential and sensitive data environment(s) storing Plaintiffs' and the Class members' PII reasonably and appropriately in order to prevent or limit the Data Breach;

g. Failing to implement and maintain reasonable data storage and retention policies and procedures with respect to the PII to ensure PII was being stored and maintained only for legitimate and useful purposes;

h. Failing to undertake reasonable and sufficient incident response measures to ensure that the ransomware attack directed toward Defendants' sensitive business information would not expose and cause disclosure and unauthorized acquisition of Plaintiffs' and the Class members' PII;

i. Failing to ensure that any and all unauthorized copies of accessed data, including Plaintiffs' and the Class members' PII was deleted, destroyed, rendered unable to be used, or returned to Plaintiffs and the Class members;

j. Failing to reasonably conduct forensic investigation into the scope, nature, and exposure of the Data Breach or to ascertain its full severity;

k. Failing to provide full disclosure, deceptively misleading consumers through false representations and misleading omissions of fact regarding the Data Breach, consumers' risk and exposure caused by the Data Brach, and the adequacy of the investigation of and response to the Data Breach; and

l. Failing to provide accurate, complete, and sufficiently detailed notice to Plaintiffs and the Class regarding the circumstances of the Data Breach, its causes, its effects, the extent of the exposure of their PII, and details regarding the disposition of Plaintiffs' and the Class members' PII at all times during the Data Breach.

425. Plaintiffs' and Class Members' willingness to entrust Defendants with their PII and financial information was predicated on the understanding that Defendants would take adequate security precautions. Moreover, only Defendants had the ability to protect their systems and the PII and financial information they stored on them from attack. Thus, Defendants had a special relationship with Plaintiffs and Class Members.

426. Plaintiffs and the Class reasonably relied on Defendants' false information and were justifiably induced to obtain Defendants' products and services in reliance thereon.

427. As a direct and proximate result of Defendants' negligent misrepresentations, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft, (ii) the loss of the opportunity of how their PII and financial information is used, (iii) the compromise, publication, and/or theft of their PII and financial information, (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and financial information, (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to, efforts spent researching how to prevent, detect, contest, and recover from embarrassment and identity theft, (vi) the continued risk to their PII and financial information, which may remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII and financial information in its continued possession, and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and financial information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

428. As a direct and proximate result of Defendants' negligent misrepresentations, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

429. Additionally, as a direct and proximate result of Defendants' negligent misrepresentations, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their PII and financial information, which remain in Defendants' possession and

are subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII and financial information in its continued possession.

THIRD CLAIM FOR RELIEF AND CAUSE OF ACTION
BREACH OF CONTRACT

On Behalf of Plaintiffs Hustle N Flow Ventures, LLC, Ayana Looney, Daniel LeFebvre, David Andrew, Erik Brook, Glenn Mulvenna, Hui Li, Joel Eagelston, Debt Cleanse Group Legal Services LLC, Josh Shi, Nathan Goldstein, Noah Bunag, R. Andre Klein, Sarbjit Dhesi, and Steven Carter, and their respective Subclasses, Against All Defendants

430. Plaintiffs restate and reallege all preceding allegations in paragraphs 1 through 391 as if fully set forth herein.

431. Plaintiffs bring this claim under the law of the Commonwealth of Massachusetts on behalf of individuals and entities that paid for LastPass accounts.

432. Defendant LastPass promises in its Personal Terms of Service:

> 4.2. l. Information Security and Certifications
> We have implemented and maintain appropriate organizational, administrative, and technical safeguards designed to protect your Content against any unauthorized access, loss, misuse, or disclosure. We also maintain a compliance program that includes independent third-party audits and certifications. You can visit our Trust & Privacy Center (http://www.lastpass.com/trust-center) to review Service-specific information about our technical and organizational security measures (located in the Technical and Organizational Measures or "TOMs" documentation), including, but not limited to, encryption use and standards, retention periods, and other helpful information.
>
> 4.2.2. Data Privacy
> We maintain a global data privacy program, designed to safeguard and responsibly handle your Content and any associated personal data we may collect and/or process on your behalf. You understand that when using the Services or interacting with our websites your personal data may be processed via equipment and resources located in the United States and other locations throughout the world. You can visit our Trust & Privacy Center (http://www.lastpass.corn/trust¬ center/privacy) to review LastPass's comprehensive privacy program, third-party frameworks, privacy policies, and applicable data processing locations and Sub¬ Processor Disclosures, as well as the TOMs.

433. Defendant LastPass promises in its Business Terms of Service:

> 4.2.1. Information Security and Certifications
> LastPass agrees to maintain appropriate organizational, administrative, and technical safeguards designed to protect your Content against any unauthorized access, loss, misuse, or disclosure, in accordance with industry standards. Additional information about LastPass's technical and organizational security measures ("TOMs"), including, but not limited to, encryption use and standards, retention periods, and other helpful information can be found in our Trust & Privacy Center (http://www.lastpass.com/trust-center), along with information regarding our independent third-party security audits and certifications.
>
> 4.2.2 Data Privacy
> While providing the Services to you, LastPass agrees to handle your Content and any associated personal data we may collect and/or process on your behalf in a responsible manner. You can v1s1t our Trust & Privacy Center (http://www.lastpass.com/trust-center/privacy) to review additional information about LastPass's' comprehensive privacy program, third-party privacy frameworks, privacy policies, and applicable data processing locations and Sub-Processor Disclosures. You understand that when using our Services or interacting with our websites your personal data may be processed via equipment and resources located in the United States and other locations throughout the world. When providing our Services, LastPass acts as a data processor, service provider, or the equivalent construct. To review and execute LastPass's Data Processing Addendum ("DPA"), please visit https://www .lastpass.com/legal-center.

434. Defendant GoTo promises in its Terms of Service:

> 4.2 Your Privacy and Security
> We maintain a global privacy and security program designed to protect your Content and any associated personal data we may collect and/or process on your behalf. You can v1s1t our Trust & Privacy Center (http://www.goto.com/company/trust) to review applicable data processing locations and Sub-Processor Disclosures, as well as Service-specific information about our technical and organizational security measures (located in the Technical and Organizational Measures or "TOMs" documentation). When providing our Services, we act as a data processor, service provider, or the equivalent construct. To review and execute our Data Processing Addendum ("DPA"), please visit https://www .goto.com/company/legal.

435. Additionally, Defendant GoTo incorporates its security measure representations into its Terms of Service, as follows:

> GoTo is dedicated to monitoring and continuously improving our security, technical and organizational measures to better protect your sensitive Customer Content. We are always evaluating industry standard practices regarding technical

> data privacy and information security and strive to meet or exceed those standards. Our security programs are comprehensive and dedicated to all facets of security.
>
> Alongside our stringent internal security controls, we hold the following trusted third-party security certifications. As part of our commitment to our subscribers, we conduct SOC 2 (type II) audits, and share out a SOC 3 report, which is a shareable version of the SOC 2. The SOC 3 reports for each applicable product, can be found and downloaded on our product resources page here.

436. Defendants breached the foregoing contractual terms resulting in the Data Breach, in one or more of the following ways:

a. Failing to conduct proper and reasonable training and due diligence over vendors and employees and data security systems, practices, and procedures;

b. Failing to conduct proper and reasonable due diligence over the employees, vendors or contractors that were the vector(s) of and/or facilitated the hackers' infiltration into the system(s) storing Plaintiffs' and Class Members' PII;

c. Failing to maintain adequate and appropriate oversight and audits on their internal data security and their employees, vendors, or contractors that were the vectors of the hackers' infiltration into the system(s) storing Plaintiffs' and the Class Members' PII;

d. Failing to adequately separate and isolate PII from publicly accessible or publicly adjacent environment(s);

e. Failing to implement and maintain adequate safeguards and procedures to prevent the unauthorized access to Plaintiffs' and Class Members' PII;

f. Failing to monitor and detect their confidential and sensitive data environment(s) storing Plaintiffs' and Class Members' PII reasonably and appropriately in order to prevent or limit the Data Breach;

g. Failing to implement and maintain reasonable data storage and retention procedures with respect to the PII to ensure the PII was being stored and maintained only for legitimate and useful purposes;

h. Failing to undertake reasonable and sufficient incident response measures to ensure that the ransomware attack directed toward Defendants' sensitive business information would not expose and cause disclosure and unauthorized acquisition of Plaintiffs' and Class Members' PII;

i. Failing to ensure that any and all unauthorized copies of accessed data, including Plaintiffs' and Class Members' PII, was deleted, destroyed, rendered unable to be used, or returned to Plaintiffs and the Class Members;

j. Failing to reasonably conduct forensic investigation into the scope, nature, and exposure of the Data Breach or to ascertain its full severity;

k. Failing to provide full disclosure, deceptively misleading consumers through false representations and misleading omissions of fact regarding the Data Breach, consumers' risk and exposure caused by the Data Breach, and the adequacy of the investigation of and response to the Data Breach; and

l. Failing to provide accurate, complete, and sufficiently detailed notification to Plaintiffs and the Class Members regarding the circumstances of the Data Breach, its causes, its effects, the extent of the exposure of their PII, and details regarding the disposition of Plaintiffs' and Class Members' PII at all times during the Data Breach.

437. All conditions precedent were performed or have occurred.

438. As a direct and proximate result of Defendants' breach of contract, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft, (ii) the loss of the opportunity of how their PII and financial information is used, (iii) the compromise, publication, and/or theft of their PII and financial information, (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and financial information, (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to, efforts spent researching how to prevent, detect, contest, and recover from embarrassment and identity theft, (vi) the continued risk to their PII and financial information, which may remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII and financial information in its continued possession, and (vii) future costs in terms of time, effort, and money

that will be expended to prevent, detect, contest, and repair the impact of the PII and financial information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

439. As a direct and proximate result of Defendants' breach of contract, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

440. Additionally, as a direct and proximate result of Defendants' breach of contract, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their PII and financial information, which remain in Defendants' possession and are subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII and financial information in its continued possession.

FOURTH CLAIM FOR RELIEF AND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT

On Behalf of All Plaintiffs
Against All Defendants

441. Plaintiffs restate and reallege all preceding allegations in paragraphs 1 through 391 as if fully set forth herein.

442. Plaintiffs bring this claim under the law of the Commonwealth of Massachusetts, in the alternative to the breach of contract claim on behalf of individuals and entities which paid for LastPass accounts, and in the first instance on behalf of individuals and entities which did not pay for LastPass accounts.

443. Through their course of conduct, Defendants, Plaintiffs, and Class Members entered into implied contracts for Defendants to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' PII and financial information.

444. Specifically, Plaintiffs entered into a valid and enforceable implied contract with Defendants when they first began using Defendants' services.

445. The valid and enforceable implied contracts to provide password and identity management services that Plaintiffs and Class Members entered into with Defendants include Defendants' promise to protect nonpublic PII entrusted to it.

446. Defendants required Plaintiffs and Class Members to provide and entrust their PII and financial information as a condition of obtaining Defendants' services.

447. Defendants solicited and invited Plaintiffs and Class Members to provide their PII and financial information as part of Defendants' regular business practices. Plaintiffs and Class Members accepted Defendants' offers and provided their PII and financial information to Defendants.

448. As a condition of their relationship with Defendants, Plaintiffs and Class Members provided and entrusted their PII and financial information to Defendants. In so doing, Plaintiffs and Class Members entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class Members if their data had been breached and compromised or stolen.

449. A meeting of the minds occurred when Plaintiffs and Class Members agreed to, and did, provide their PII and financial information to Defendants, in exchange for, amongst other things, the protection of their PII and financial information.

450. By entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations and were consistent with industry standards.

451. Under these implied contracts, Defendants promised and were obligated to: (a) provide password and identity management services to Plaintiffs and Class Members; and (b) protect Plaintiffs and the Class Members' PII provided to obtain such benefits of such services. In exchange, Plaintiffs and Class Members agreed to turn over their PII to LastPass.

452. Both the provision of password and identity management services and the protection of Plaintiffs and Class Members' PII were material aspects of these implied contracts.

453. The implied contracts for the provision of password and identity management services, including but not limited to, the maintenance of the privacy of Plaintiffs and Class Members' PII, are also acknowledged, memorialized, and embodied in Defendants' Terms of Service.

454. Defendants' express representations, including, but not limited to, the express representations found in its Terms of Service, memorialize and embody the implied contractual obligations requiring Defendants to implement data security adequate to safeguard and protect the privacy of Plaintiffs and Class Members, and to protect the privacy of Plaintiffs' and Class Members' PII.

455. Users of password management services value their privacy and the ability to keep their PII associated with obtaining such services. Plaintiffs and Class Members would not have entrusted their PII to Defendants and entered into these implied contracts with Defendants without an understanding that their PII would be safeguarded and protected; nor would they have entrusted

their PII to Defendants in the absence of the implied promise by Defendants to monitor the PII and to ensure that it adopted reasonable administrative and data security measures.

456. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendants.

457. Defendants breached the implied contracts they made with Plaintiffs and Class Members by failing to safeguard and protect their PII and financial information and by failing to provide timely and accurate notice to them that their PII and financial information was compromised as a result of the Data Breach.

458. As a direct and proximate result of Defendants' breach of the implied contract, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft, (ii) the loss of the opportunity of how their PII and financial information is used, (iii) the compromise, publication, and/or theft of their PII and financial information, (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and financial information, (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to, efforts spent researching how to prevent, detect, contest, and recover from embarrassment and identity theft, (vi) the continued risk to their PII and financial information, which may remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII and financial information in its continued possession, and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and

financial information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

459. As a direct and proximate result of Defendants' breach of the implied contract, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

460. Additionally, as a direct and proximate result of Defendants' breach of the implied contract, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their PII and financial information, which remain in Defendants' possession and are subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII and financial information in its continued possession.

461. Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

462. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen its data security systems and monitoring procedures; and (ii) submit to future bi- annual audits of those systems and monitoring procedures.

FIFTH CLAIM FOR RELIEF AND CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY

On Behalf of All Plaintiffs
Against All Defendants

463. Plaintiffs restate and reallege all preceding allegations in paragraphs 1 through 391 as if fully set forth herein.

464. Plaintiffs bring this claim under the law of the Commonwealth of Massachusetts.

465. Plaintiffs and Class Members have an interest, both equitable and legal, in the PII that was conveyed to and collected, stored, and maintained by Defendants and which was ultimately compromised by unauthorized cybercriminals as a result of the Data Breach.

466. Defendants, in taking possession of this highly sensitive information, formed a special relationship with its customers, including Plaintiffs and the Class.

467. Plaintiffs and the Class Members put their trust and confidence in Defendants' judgment, honesty, and integrity in protecting their PII and the various accounts that could be accessed through use (or misuse) of that PII.

468. Defendants knew that Plaintiffs and Class Members were relying on Defendants, and accepted this trust and confidence when they accepted PII from Plaintiffs and Class Members.

469. As a result of that special relationship, Defendants were provided with and stored private and valuable information belonging to Plaintiffs and the Class, which Defendants were required by law and industry standards to maintain in confidence.

470. In light of the special relationship between Defendants and Plaintiffs and Class Members, whereby Defendants became a guardian of Plaintiffs' and Class Members' PII, Defendants undertook a fiduciary duty to act primarily for the benefit of its customers, including Plaintiffs and Class Members, for the safeguarding of Plaintiffs' and Class Members' PII.

471. Defendants had a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of this relationship, in particular, to keep secure Plaintiffs' and Class members' PII and to maintain the confidentiality of their PII.

472. Defendants owed a duty to Plaintiffs and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in its

possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

473. Plaintiffs and Class Members have a privacy interest in their personal and proprietary matters and Defendants had a duty not to disclose or allow unauthorized access to such confidential information.

474. Plaintiffs' and Class Members' PII is not generally known to the public and is confidential by nature. Moreover, Plaintiffs and Class Members did not consent to nor authorize Defendants to release or disclose their PII to unknown criminal actors.

475. Defendants breached their fiduciary duty to Plaintiffs and Class Members when Plaintiffs' and Class Members' PII was disclosed to unknown criminal hackers by way of Defendants' own acts and omissions, as alleged herein.

476. Defendants knowingly breached their fiduciary duties by failing to safeguard Plaintiffs' and Class Members' PII, including by, among other things:

a. mismanaging their system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of the PII;

b. mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks;

c. failing to design and implement information safeguards to control these risks;

d. failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures;

e. failing to evaluate and adjust its information security program in light of the circumstances alleged herein;

f. failing to detect the Data Breach at the time it began or within a reasonable time thereafter and give adequate notice to Plaintiffs and Class Members thereof;

g. failing to follow its own privacy policies and practices published to its customers;

h. storing PII in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and

i. making an unauthorized and unjustified disclosure and release of Plaintiffs' and Class Members' PII to a criminal third party.

477. But for Defendants' wrongful breach of its fiduciary duties owed to Plaintiffs and Class Members, their privacy would not have been compromised and their PII would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by and/or viewed by unauthorized third parties.

478. As a direct and proximate result of Defendants' breach of its fiduciary duties, Plaintiffs and Class Members have suffered or will suffer injuries, including but not limited to, the following: loss of their privacy and confidentiality of their PII; theft of their PII; costs associated with the detection and prevention of fraud and unauthorized use of their PII; costs associated with purchasing credit monitoring and identity theft protection services; costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Defendants' Data Breach-including finding fraudulent charges, enrolling in credit monitoring and identity theft protection services, and filing reports with the police and FBI; the imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals; damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiffs and Class Members' data against theft and not allow access and misuse of their data by others; continued risk of exposure to hackers and thieves of their PII, which remains in Defendants' possession and

is subject to further breaches so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data; and/or mental anguish accompanying the loss of confidence and disclosure of their PII.

479. Defendants breached their fiduciary duty to Plaintiffs and Class Members when they made an unauthorized release and disclosure of their confidential PII and, accordingly, it would be inequitable for Defendants to retain the benefits they have received at Plaintiffs' and Class Members' expense.

480. Plaintiffs and Class Members are entitled to damages and/or disgorgement or restitution, in an amount to be proven at trial.

SIXTH CLAIM FOR RELIEF AND CAUSE OF ACTION
BREACH OF COVENANT OF GOOD FAITH AND FAIR DEALING

On Behalf of All Plaintiffs
Against All Defendants

481. Plaintiffs restate and reallege all preceding allegations in paragraphs 1 through 391 as if fully set forth herein.

482. Plaintiffs bring this claim under the law of the Commonwealth of Massachusetts.

483. Every contract in this state has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

484. Plaintiffs and Class Members have complied with and performed all conditions of their contracts with Defendants.

485. Defendants breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PII and financial information, failing to timely and accurately disclose the Data Breach to Plaintiffs and Class

Members and continued acceptance of PII and financial information and storage of other personal information after Defendants knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

486. Defendant acted in bad faith and/or with malicious motive in denying Plaintiffs and Class Members the full benefit of their bargains as originally intended by the parties.

487. As a direct and proximate result of Defendants' breach of the implied covenant of good faith and fair dealing, Plaintiffs and the Class Members have suffered injury and are entitled to damages, including restitution, unjust enrichment and disgorgement in an amount to be proven at trial, declaratory and injunctive relief, and attorney fees, costs, and expenses.

SEVENTH CLAIM FOR RELIEF AND CAUSE OF ACTION
UNJUST ENRICHMENT

On Behalf of Plaintiffs Hustle N Flow Ventures, LLC, Ayana Looney, Daniel LeFebvre, David Andrew, Erik Brook, Glenn Mulvenna, Joel Eagelston, Debt Cleanse Group Legal Services LLC, Josh Shi, Nathan Goldstein, R. Andre Klein, Sarbjit Dhesi, and Steven Carter, and their respective Subclasses, Against All Defendants

488. Plaintiffs restate and reallege all preceding allegations in paragraphs 1 through 391 as if fully set forth herein.

489. Plaintiffs bring this claim under the law of the Commonwealth of Massachusetts on behalf of individuals and entities which paid for LastPass accounts.

490. This claim is brought in the alternative to the other claims.

491. By their wrongful acts and omissions described herein, Defendants have obtained a benefit by unduly taking advantage of Plaintiffs and Class Members.

492. Defendants, prior to and at the time Plaintiffs and Class Members entrusted their PII and financial information to Defendants for the purpose of obtaining services, caused Plaintiffs and Class Members to reasonably believe that Defendants would keep such PII and financial information secure.

493. Defendants were aware, or should have been aware, that reasonable consumers would have wanted their PII and financial information kept secure and would not have contracted with Defendants, directly or indirectly, had they known that Defendants' information systems were sub-standard for that purpose.

494. Defendants were also aware that, if the substandard condition of and vulnerabilities in their information systems were disclosed, it would negatively affect Plaintiffs' and Class Members' decision to seek services therefrom.

495. Defendants failed to disclose facts pertaining to their substandard information systems, defects, and vulnerabilities therein before Plaintiffs and Class Members made their decisions to make purchases, engage in commerce therewith, and seek services or information. Instead, Defendants suppressed and concealed such information. By concealing and suppressing that information, Defendants denied Plaintiffs and Class Members the ability to make a rational and informed purchasing decision and took undue advantage of Plaintiffs and Class Members.

496. Defendants were unjustly enriched at the expense of Plaintiffs and Class Members. Defendants received profits, benefits, and compensation, in part, at the expense of Plaintiffs and Class Members. By contrast, Plaintiffs and Class Members did not receive the benefit of their bargain because they paid for products and/or services that did not satisfy the purposes for which they bought/sought them.

497. Since Defendants' profits, benefits and other compensation were obtained by improper means, Defendants are not legally or equitably entitled to retain any of the benefits, compensation or profits it realized from these transactions.

498. Plaintiffs and Class Members seek an Order of this Court requiring Defendants to refund, disgorge, and pay as restitution any profits, benefits, or other compensation obtained by

Defendants from their wrongful conduct and/or the establishment of a constructive trust from which Plaintiffs and Class Members may seek restitution.

EIGHTH CLAIM FOR RELIEF AND CAUSE OF ACTION
DECLARATORY AND INJUNCTIVE RELIEF

On Behalf of All Plaintiffs
Against All Defendants

499. Plaintiffs restate and reallege all preceding allegations in paragraphs 1 through 391 as if fully set forth herein.

500. Pursuant to state and federal law, this Court is authorized to enter a judgment making binding declarations of right, duty, status and other legal relations between parties. The Court also has broad authority to restrain acts, such as here, that are tortious and violate the terms of the regulations described in this Complaint.

501. An actual controversy has arisen in the wake of the Data Breach regarding LastPass's present and prospective duties to reasonably safeguard users' PII and whether LastPass is maintaining data security measures adequate to protect the Class Members, including Plaintiffs, from further data breaches that compromise their PII, including but not limited to, their respective customer vaults.

502. Plaintiffs allege that LastPass's data-security measures remain inadequate. LastPass denies these allegations and attempts to cast the blame of the harm suffered by Plaintiffs and Class Members upon Plaintiffs and Class Members themselves. In addition, Plaintiffs and the Class continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII and continued fraudulent activity against them will occur in the future.

503. Pursuant to its authority under the Massachusetts Declaratory Judgment Act, as well as the Federal Rules of Civil Procedure, and other applicable law, Plaintiffs ask the Court to enter a judgment declaring, among other things, the following: (i) LastPass owes a duty to secure consumers' PII and to timely notify consumers of a data breach; and (ii) LastPass is in breach of these legal duties by failing to employ reasonable measures to secure consumers' PII in its possession and control.

504. Plaintiffs further ask the Court to issue corresponding prospective injunctive relief requiring LastPass to employ adequate security protocols consistent with law and industry standards to protect consumers' PII from future data breaches.

505. If an injunction is not issued, Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at LastPass. The risk of another such breach is real, immediate, and substantial. If another breach at LastPass occurs, Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and Class Members will be forced to bring multiple lawsuits to rectify the same misconduct.

506. The hardship to Class Members if an injunction does not issue exceeds the hardship to LastPass if an injunction is issued. Among other things, if a similar data breach occurs again due to the repeated misconduct of LastPass, Class Members will likely be subjected to substantial hacking and phishing attempts and other damage, in addition to the damages already suffered. On the other hand, the cost to LastPass of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and LastPass has pre-existing legal obligations to employ such measures.

507. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing additional data breaches at LastPass, thus eliminating the additional injuries that would result to Class Members and the millions of consumers whose personal and confidential information would be further compromised.

CLAIMS ON BEHALF OF THE NATIONWIDE CLASS AND MASSACHUSETTS SUBCLASS

NINTH CLAIM FOR RELIEF AND CAUSE OF ACTION
MASSACHUSETTS CONSUMER PROTECTION ACT
MASS. GEN. LAWS ANN. CH. 93A, §§ 1, *et seq*.

On Behalf of All Plaintiffs
Against All Defendants

508. Plaintiffs restate and reallege all preceding allegations in paragraphs 1 through 391 as if fully set forth herein.

509. This claim is brought individually under the laws of Massachusetts and on behalf of all other natural persons whose PII was compromised.

510. Defendants, Plaintiff and Class Members are "persons" as meant by Mass. Gen. Laws. Ann. Ch. 93A, § 1(a).

511. LastPass and GoTo operate in "trade or commerce" as meant by Mass. Gen. Laws Ann. Ch. 93A, § 1(b).

512. Defendants advertised, offered, or sold goods or services in Massachusetts and engaged in trade or commerce directly or indirectly affecting the people of Massachusetts, as defined by Mass. Gen. Laws Ann. Ch. 93A, § 1(b).

513. Plaintiffs sent written demands for relief on behalf of themselves and Class Members pursuant to Mass. Gen. Laws Ann. Ch. 93A § 9(3)—including, but not limited to on

January 18 and February 10, 2023. Last Pass did not respond with a reasonable offer of relief to Plaintiffs and the Class.

514. Defendants engaged in unfair methods of competition and unfair and deceptive acts and practices in the conduct of trade or commerce, in violation of Mass. Gen. Laws Ann. Ch. 93A, § 2(a), including by:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05;

f. Failing to timely and adequately notify Plaintiffs and Class Members of the Data Breach;

g. Misrepresenting that certain sensitive PII was not accessed during the Data Breach, when it was;

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' PII; and

i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05.

515. LastPass's acts and practices were "unfair" because they fall within the penumbra of common law, statutory, and established concepts of unfairness, given that LastPass solely held the true facts about its inadequate security for PII, which Plaintiffs and Class Members could not independently discover.

516. LastPass's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and Class Members, that their PII was not exposed and misled Plaintiffs and Class Members into believing they did not need to take actions to secure their identities.

517. Consumers could not have reasonably avoided injury because LastPass's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, LastPass created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

518. LastPass's inadequate data security had no countervailing benefit to consumers or to competition. LastPass intended to mislead Plaintiffs and Class Members and induce them to rely on its misrepresentations and omissions. LastPass's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of LastPass's data security and ability to protect the confidentiality of consumers' PII.

519. LastPass acted intentionally, knowingly, and maliciously to violate Massachusetts' Consumer Protection Act, and recklessly disregarded Plaintiffs' and Class Members' rights.

520. As a direct and proximate result of LastPass's unfair and deceptive trade practices, Plaintiffs and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

521. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including actual damages, double or treble damages, injunctive or other equitable relief, and attorneys' fees and costs.

TENTH CLAIM FOR RELIEF AND CAUSE OF ACTION
MASS. GEN. LAWS ANN. CH. 93A, §§ 11, *et seq.*

On Behalf of Plaintiffs HNF and Debt Cleanse and the Nationwide Business Class Against All Defendants

522. Plaintiffs restate and reallege all preceding allegations in paragraphs 1 through 391 as if fully set forth herein.

523. This cause of action is brought on behalf of Plaintiffs HNF and Debt Cleanse on behalf of themselves and the Nationwide Business Class.

524. Plaintiffs HNF and Debt Cleanse are engaged in trade or commerce, and have suffered loss of money or property due to the use of an unfair method of competition or an unfair or deceptive business practice by Defendants, as described throughout this Complaint.

525. The actions and transactions constituting the unfair or deceptive act or practice occurred primarily and substantially within Massachusetts. The center of gravity of Defendants' deceptive and unfair acts and practices is within the Commonwealth of Massachusetts.

526. As a result of Defendants' deceptive and unfair acts and practices, Plaintiffs HNF, Debt Cleanse, and the Nationwide Business Class members were injured.

CLAIMS ON BEHALF OF STATE SUBCLASSES

527. Plaintiffs bring the following causes of action in the event they provide additional relief beyond that provided by Massachusetts state law.

CLAIMS ON BEHALF OF THE ARIZONA SUBCLASS

ELEVENTH CLAIM FOR RELIEF AND CAUSE OF ACTION
ARIZONA CONSUMER FRAUD ACT, A.R.S. §§ 44-1521, *et seq.*

On Behalf of Plaintiff Joel Eagelston and the Arizona Subclass
Against Defendant LastPass

528. Plaintiffs restate and reallege all preceding allegations in paragraphs 1 through 391 as if fully set forth herein.

529. Plaintiff Joel Eagelston ("Plaintiff") brings this action on behalf of himself and the Arizona Subclass.

530. LastPass is a "person" as defined by A.R.S. § 44-1521(6).

531. LastPass advertised, offered, or sold goods or services in Arizona and engaged in trade or commerce directly or indirectly affecting the people of Arizona.

532. LastPass engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts affecting the people of Arizona in connection with the sale and advertisement of "merchandise" (as defined in Arizona Consumer Fraud Act, A.R.S. § 44-1521(5)) in violation of A.R.S. § 44-1522(A)).

533. LastPass's unfair and deceptive acts and practices included:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and properly improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or properly secure Plaintiff's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

534. LastPass's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of LastPass's data security and ability to protect the confidentiality of consumers' PII.

535. LastPass intended to mislead Plaintiff and Arizona Subclass Members and induce them to rely on its misrepresentations and omissions.

536. Had LastPass disclosed to Plaintiff and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, LastPass would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. LastPass was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and Subclass Members. LastPass accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly,

Plaintiff and Subclass Members acted reasonably in relying on LastPass's misrepresentations and omissions, the truth of which they could not have discovered.

537. LastPass acted intentionally, knowingly, and maliciously to violate Arizona's Consumer Fraud Act, and recklessly disregarded Plaintiff's and Arizona Subclass Members' rights. LastPass is an industry leader in the sale of online security and has been the object of multiple security breaches dating back to at least 2011, including when a cyber attacker gained sustained access to its development environment in or around August 2022. Taken together, LastPass was on notice that its security and privacy protections were inadequate and had remained inadequate for the last 13 years.

538. As a direct and proximate result of LastPass's unfair and deceptive acts and practices, Plaintiff and Arizona Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for LastPass's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

539. Plaintiff and Arizona Subclass Members seek all monetary and non-monetary relief allowed by law, including compensatory damages; disgorgement; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE CALIFORNIA SUBCLASS

TWELFTH CLAIM FOR RELIEF AND CAUSE OF ACTION CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE § 17200, *et seq.*

On Behalf of Plaintiffs Ayana Looney, Noah Bunag, Sarbjit Dhesi, Erik Brook and the California Subclass Against Defendant LastPass

540. Plaintiffs restate and reallege all preceding allegations in paragraphs 1 through 391 as if fully set forth herein.

541. Plaintiffs Ayana Looney, Noah Bunag, Sarbjit Dhesi, and Erik Brook ("Plaintiffs") bring this claim on behalf of themselves and the California Subclass.

542. LastPass is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

543. LastPass violated Cal. Bus. & Prof. Code §§ 17200, *et seq*. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

544. LastPass's unlawful acts, unfair acts, and deceptive acts and practices include:

a. LastPass failed to implement and maintain reasonable security measures to protect Plaintiffs and the California Subclass Members from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. LastPass failed to:

1.

i. Secure their website;

ii. Secure access to their servers;

iii. Comply with industry-standard security practices;

iv. Employ adequate network segmentation;

v. Implement adequate system and event monitoring;

vi. Utilize modern payment systems that provide more security against intrusion;

vii. Install updates and patches in a timely manner, and

viii. Implement the systems, policies, and procedures necessary to prevent this type of data breach.

c. LastPass failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiffs and the California Subclass Members whose PII has been compromised;

d. LastPass's failure to implement and maintain reasonable security measures also was contrary to legislatively declared public policy that seeks to protect consumer data and ensure that entities that are trusted with its use appropriate security measures. These policies are reflected in laws, including the FTCA, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.81.5 et seq., and California's Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq.;

e. LastPass's failure to implement and maintain reasonable security measures also led to substantial injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because Plaintiffs and the California Subclass Members could not know of LastPass's inadequate security, consumers could not have reasonably avoided the harms that LastPass caused;

f. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs and the California Subclass Members' PII, including by implementing and maintaining reasonable security measures;

g. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the California Subclass Members' PII, including duties imposed by the FTCA, 15 U.S.C § 45; California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq.; and California's Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq.;

h. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and the California Subclass Members' PII;

i. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the California Subclass Members' PII, including duties imposed by the FTCA, 15 U.S.C § 45; California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq.; and California's Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq.;

j. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82; and

k. Other ways to be discovered and proved at trial.

545. LastPass's representations and material omissions of fact, as alleged herein, to Plaintiffs and the California Subclass Members were material because they were likely to deceive reasonable consumers about the adequacy of LastPass's data security and ability to protect the privacy of consumers' PII.

546. LastPass intended to mislead Plaintiffs and the California Subclass Members and induce them to rely on its misrepresentations and material omissions of fact as alleged herein.

547. Had LastPass disclosed to Plaintiffs and the California Subclass Members that its data systems were not secure and, thus, vulnerable to attack, LastPass would have been unable to continue in business, and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, LastPass received, maintained, and compiled Plaintiffs' and the California Subclass Members' PII as part of the services and goods LastPass provided without advising Plaintiffs and the California Subclass Members that LastPass's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs and the California Subclass Members. Accordingly, Plaintiffs and the California Subclass Members acted reasonably in relying on LastPass's misrepresentations and material omissions of fact, the truth of which they could not have discovered.

548. LastPass acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's' and the California Subclass Members' rights.

549. As a direct and proximate result of LastPass's unfair, unlawful, and fraudulent acts and practices, Plaintiffs and the California Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages as described herein and as will be proved at trial.

550. Plaintiffs and the California Subclass Members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from LastPass's unfair, unlawful, and fraudulent business practices or use of their PII; declaratory relief; injunctive relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; and other appropriate equitable relief.

551. Plaintiffs and the California Subclass Members also seek injunctive relief requiring LastPass to, e.g., (a) strengthen their data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) continue to provide adequate credit monitoring to all California Class Members. Plaintiffs' and the California Subclass Members' legal remedies are inadequate to provide this requested injunctive relief.

THIRTEENTH CLAIM FOR RELIEF AND CAUSE OF ACTION
CALIFORNIA CONSUMER LEGAL REMEDIES ACT,
CAL. CIV. CODE §§ 1750, *et seq.*

On Behalf of Plaintiffs Ayana Looney, Noah Bunag, Sarbjit Dhesi, Erik Brook and the California Subclass Against Defendant LastPass

552. Plaintiffs restate and reallege all preceding allegations in paragraphs 1 through 391 as if fully set forth herein.

553. Plaintiffs Ayana Looney, Noah Bunag, Sarbjit Dhesi, and Erik Brook ("Plaintiffs") bring this claim on behalf of themselves and the California Subclass.

554. Plaintiffs and the California Subclass Members are residents of California.

555. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, et seq. ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

556. LastPass is a "person" as defined by Civil Code §§ 1761€ and 1770 and have provided "services" as defined by Civil Code §§ 1761(b) and 1770.

557. Plaintiffs and the California Subclass are "consumers" as defined by Civil Code §§ 1761(d) and 1770 and have engaged in a "transaction" as defined by Civil Code §§ 1761€ and 1770.

558. LastPass's acts and practices were intended to and did result in the sales of products and services to Plaintiffs and the California Subclass Members in violation of Civil Code § 1770, including by:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade when they were not;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

559. LastPass's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of their LastPass's data security and ability to protect the confidentiality of consumers' PII.

560. Had LastPass disclosed to Plaintiffs and the California Subclass Members that their data systems were not secure and, thus, were vulnerable to attack, they would have been unable to continue in business and they would have been forced to adopt reasonable data security measures and comply with the law. LastPass was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiffs and the California Subclass Members. LastPass accepted the responsibility of protecting the data but kept the inadequate state of their security controls secret from the public. Accordingly, Plaintiffs and the California Subclass Members acted reasonably in

relying on LastPass's misrepresentations and omissions, the truth of which they could not have discovered.

561. LastPass advertised that it would provide a secure and safe place for customers' information, a service for which LastPass charged consumers as much as $36 per year.

562. On June 9, 2023, counsel for Plaintiffs provided written notice to LastPass and GoTo by email (pursuant to an agreement of counsel to accept service of the notice on behalf of Defendants by email) of their intent to pursue claims under the California Consumers Legal Remedies Act and an opportunity for LastPass to cure. LastPass's Plaintiff's' written notice set forth, and incorporated by reference to prior filed complaints regarding the Data Breach, the violations of LastPass's duty to implement and maintain reasonable security procedures and practices alleged in this Consolidated Complaint.

563. Plaintiff's' June 9, 2023, written notice substantially complied with California Civil Code Section 1782's written notice requirement. In addition, Defendants received written notice of the factual bases of this cause of action and others when plaintiffs in multiple actions that were filed in multiple jurisdictions served Defendants with complaints in connection with the Data Breach. Those complaints were filed more than 100 days ago, prior to the consolidation of the actions in the United States District Court for the District of Massachusetts.[131]

[131] These actions included *Debt Cleanse Group Legal Services, LLC.*, No. l:22-cv-12047-PBS (D. Mass.); *John Doe*, No. 1:23-CV-10004-PBS (D. Mass.); *R. Andre Klein*, No. l:23-cv-10122-PBS (D. Mass); *Steven Carter*, No. l:23-cv-10092-DJC (D. Mass); *Nathan Goldstein*, No. l:23-cv-10320-PBS (D. Mass); *David Andrew*, No. l:23-cv-10338-PBS (D. Mass); *Alan Murphy, Jr.*, No. l:23-cv-10415-PBS (D. Mass); *Denise Remhoff*, No. l:23-cv-10493-PBS (D. Mass), *Steven Linthicum*, No. l:23-cv-10502-PBS (D. Mass); and *John Doe*, No. CGC-23-604214 (Cal. S.F. Super. Ct.)

564. These actions contained similar factual allegations to those giving rise to this cause of action, and LastPass has therefore had ample opportunity to investigate the basis of this action and pursue settlement discussions.

565. To date, LastPass has taken no action to remedy their misconduct or otherwise address the violations outlined in the written notice sent by Plaintiff's counsel. In response to the June 9, 2023 written notice, LastPass disputes that it has taken no action to remedy its misconduct or address the violations outlined in the written notice sent by Plaintiffs, but offered no additional relief. Plaintiffs' and the California Subclass Members' harms are ongoing, and those harms have not been redressed by LastPass; Plaintiffs have not been compensated for injuries suffered due to LastPass's misconduct; and LastPass has offered no proof that they have secured Plaintiffs' PII or otherwise corrected their inadequate security measures in contravention of various state laws including the CLRA. Further, to the extent Plaintiffs' and the California Subclass Members' PII lost to the Data Breach is irrecoverable, it is impossible for LastPass to cure its violations of law.

566. As a direct and proximate result of LastPass's violations of California Civil Code § 1770, Plaintiffs and the California Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for LastPass's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

567. Plaintiffs and the California Subclass seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

FOURTEENTH CLAIM FOR RELIEF AND CAUSE OF ACTION
CALIFORNIA CUSTOMER RECORDS ACT ("CCRA"),
CAL. CIV. CODE § 1798.80, *et seq.*

On Behalf of Plaintiffs Ayana Looney, Noah Bunag, Sarbjit Dhesi, Erik Brook and the California Subclass Against Defendant LastPass

568. Plaintiffs restate and reallege all preceding allegations in paragraphs 1 through 391 as if fully set forth herein.

569. Plaintiffs Ayana Looney, Noah Bunag, Sarbjit Dhesi, and Erik Brook ("Plaintiffs") bring this claim on behalf of themselves and the California Subclass.

570. Plaintiffs and Subclass Members are residents of California.

571. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code §1798.81.5, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

572. LastPass is a business that maintains PII about Plaintiff and California Subclass Members within the meaning of Cal. Civ. Code §1798.81.5.

573. As a direct and proximate result of LastPass's violations of the Cal. Civ. Code §1798.81.5, Plaintiffs and California Subclass members suffered damages, as described above and as will be proven at trial.

574. Plaintiffs and California Subclass members seek relief under Cal. Civ. Code §1798.84, including actual damages, civil penalties, injunctive relief, and reasonable attorneys' fees and costs.

FIFTEENTH CLAIM FOR RELIEF AND CAUSE OF ACTION
CALIFORNIA CONSUMER PRIVACY ACT ("CCPA"),
CAL. CIV. CODE §§ 1798.100, *et seq.*

On Behalf of Plaintiffs Ayana Looney, Noah Bunag, Sarbjit Dhesi, Erik Brook and the California Subclass Against Defendant LastPass

575. Plaintiffs restate and reallege all preceding allegations in paragraphs 1 through 391 as if fully set forth herein.

576. Plaintiffs Ayana Looney, Noah Bunag, Sarbjit Dhesi, and Erik Brook ("Plaintiffs") bring this claim on behalf of themselves and the California Subclass

577. Plaintiffs and Subclass Members are residents of California.

578. LastPass is a corporation organized or operated for the profit or financial benefit of its owners. LastPass collects consumers' personal information ("PII" for purposes of this Count) as defined in Cal. Civ. Code § 1798.140.

579. LastPass violated § 1798.150 of the CCPA by failing to prevent Plaintiffs' and Subclass Members' unencrypted PII from unauthorized access and exfiltration, theft, or disclosure as a result of LastPass's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

580. LastPass has a duty to implement and maintain reasonable security procedures and practices to protect Plaintiffs' and Subclass Members' PII. As detailed herein, LastPass failed to do so.

581. As a direct and proximate result of LastPass's acts, Plaintiffs' and Subclass Members' PII, including full names, email addresses, postal addresses, telephone numbers, dates

of birth, Social Security numbers, payment card information, and other financial information, was subjected to unauthorized access and exfiltration, theft, or disclosure.

582. Plaintiffs and Subclass Members seek injunctive or other equitable relief to ensure LastPass hereinafter properly safeguards customers' PII by implementing reasonable security procedures and practices. Such relief is particularly important because LastPass continues to hold customers' PII, including Plaintiffs' and Subclass Members' PII. Plaintiff and Subclass Members have an interest in ensuring that their PII is reasonably protected, and LastPass has demonstrated a pattern of failing to properly safeguard this information, as evidenced by its multiple failures to notify Plaintiffs of its data breach and to take appropriate remedial steps post breach.

583. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by LastPass and third parties with similar inadequate security measures.

584. On January 16, 2023, counsel for Plaintiffs provided written notice via certified mail to LastPass to its registered agent in Massachusetts of their intent to pursue claims under the California Consumer Privacy Act and an opportunity for LastPass to cure. On February 21, 2023, counsel for Plaintiffs provided written notice to LastPass and GoTo by delivering a notice letter to counsel for Defendants pursuant to an agreement between counsel to accept email service of the letter. Plaintiffs' written notice set forth the violations of LastPass's duty to implement and maintain reasonable security procedures and practices alleged in this Consolidated Complaint.

585. The January 16, 2023, and February 21, 2023, written notices, sent on behalf of a putative class of California residents, substantially complied with California Civil Code, Section 1798.150's written notice requirement. In addition, LastPass received written notice of the factual bases of this cause of action and others when the plaintiffs in multiple actions that were filed in

multiple jurisdictions served LastPass with complaints in connection with the Data Breach. Those complaints were filed more than 100 days ago, prior to the consolidation of the actions in the United States District Court for the District of Massachusetts.[132]

586. These actions contained similar factual allegations to those giving rise to this cause of action, and LastPass has therefore had ample opportunity to investigate the basis of this action and pursue settlement discussions.

587. Additionally, after these actions were consolidated by this Court, counsel for Plaintiffs provided, on June 9, 2023, a written notice letter to LastPass and GoTo by email (pursuant to an agreement of counsel to accept service of the notice on behalf of Defendants by email) of their intent to pursue the same claims, in addition to claims under various state statutes.

588. To date, LastPass has taken no action to remedy its misconduct or otherwise address the violations outlined in the written notice sent by Plaintiffs' counsel.

589. Plaintiffs and the California Subclass seek statutory damages of between $100 and $750 per customer per violation or actual damages, whichever is greater, as well as all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE FLORIDA SUBCLASS

SIXTEENTH CLAIM FOR RELIEF AND CAUSE OF ACTION
FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT
FLA. STAT. §§ 501.201, *et seq.*

[132] These actions included *Debt Cleanse Group Legal Services, LLC.*, No. l:22-cv-12047-PBS (D. Mass.); *John Doe*, No. 1:23-CV-10004-PBS (D. Mass.); *R. Andre Klein*, No. l:23-cv-10122-PBS (D. Mass); *Steven Carter*, No. l:23-cv-10092-DJC (D. Mass); *Nathan Goldstein*, No. l:23-cv-10320-PBS (D. Mass); *David Andrew*, No. l:23-cv-10338-PBS (D. Mass); *Alan Murphy, Jr.*, No. l:23-cv-10415-PBS (D. Mass); *Denise Remhoff*, No. l:23-cv-10493-PBS (D. Mass), *Steven Linthicum*, No. l:23-cv-10502-PBS (D. Mass); and *John Doe*, No. CGC-23-604214 (Cal. S.F. Super. Ct.).

On Behalf of Plaintiffs Hustle N Flow Ventures, LLC and Glenn Mulvenna and the Florida Subclass Against Defendant LastPass

590. Plaintiffs restate and reallege all preceding allegations in paragraphs 1 through 391 as if fully set forth herein.

591. Plaintiffs HNF and Glenn Mulvenna ("Plaintiffs") bring this claim on behalf of themselves and the Florida Subclass against Defendant LastPass.

592. Plaintiffs and Florida Subclass Members are "consumers" as defined by Fla. Stat. § 501.203.

593. LastPass advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

594. LastPass engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2);

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2).

595. LastPass's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of LastPass's data security and ability to protect the confidentiality of consumers' PII.

596. Had LastPass disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, were vulnerable to attack, LastPass would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. LastPass was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiffs and Subclass Members. LastPass accepted the responsibility of protecting the data but kept the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and Subclass Members acted reasonably in relying on LastPass's misrepresentations and omissions, the truth of which they could not have discovered.

597. As a direct and proximate result of LastPass's unconscionable, unfair, and deceptive acts and practices, Plaintiffs and Florida Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for LastPass's

services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

598. Plaintiffs and Florida Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages under Fla. Stat. § 501.211; declaratory and injunctive relief; reasonable attorneys' fees and costs, under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE ILLINOIS SUBCLASS

SEVENTEENTH CLAIM FOR RELIEF AND CAUSE OF ACTION ILLINOIS PERSONAL INFORMATION PROTECTION ACT 815 ILL. COMP. STAT. §§ 530/10(A), *et seq.*

On Behalf of Plaintiffs Erik Brook, David Andrew, Josh Shi, Hui Li, and Debt Cleanse Group Legal Services LLC and the Illinois Subclass Against Defendant LastPass

599. Plaintiffs restate and reallege all preceding allegations in paragraphs 1 through 391 as if fully set forth herein.

600. Plaintiffs Erik Brook, David Andrew, Josh Shi, Hui Li, and Debt Cleanse ("Plaintiffs") bring this claim on behalf of themselves and the Illinois Subclass.

601. The Illinois Plaintiffs identified above ("Plaintiffs" for purposes of this Count), individually and on behalf of the Illinois Subclass, repeat and re-allege the factual allegations set forth in the foregoing paragraphs and incorporate the same as if set forth herein.

602. As a publicly held corporation which handles, collects, disseminates, and otherwise deals with nonpublic personal information (for the purpose of this count, "PII"), LastPass is a Data Collector as defined in 815 Ill. Comp. Stat. § 530/5.

603. Plaintiffs' and Illinois Subclass Members' PII includes "personal information" as defined by 815 Ill. Comp. Stat. § 530/5.

604. LastPass is required to give immediate notice of a breach of a security system to owners of PII which LastPass does not own or license, including Plaintiffs and Illinois Subclass Members, pursuant to 815 Ill. Comp. Stat. § 530/10(b).

605. By failing to give immediate notice to Plaintiffs, LastPass violated 815 Ill. Comp. Stat. § 530/10(b).

606. LastPass is required to notify Plaintiffs and Illinois Subclass Members of a breach of its data security system which may have compromised PII which LastPass owns or licenses in the most expedient time possible and without unreasonable delay pursuant to 815 Ill. Comp. Stat. § 530/10(a).

607. By failing to disclose the Data Breach to Plaintiffs and Illinois Subclass Members in the most expedient time possible and without unreasonable delay, LastPass violated 815 Ill. Comp. Stat. § 530/10(a).

608. Pursuant to 815 Ill. Comp. Stat. § 530/20, a violation of 815 Ill. Comp. Stat. § 530/10(a) constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act.

609. As a direct and proximate result of LastPass's violations of 815 Ill. Comp. Stat. § 530/10(a), Plaintiffs and Illinois Subclass Members suffered damages, as described above.

610. Plaintiffs and Illinois Subclass Members seek relief under 815 Ill. Comp. Stat. § 510/3 for the harm they suffered because of LastPass's willful violations of 815 Ill. Comp. Stat. § 530/10(a), including actual damages, equitable relief, costs, and attorneys' fees.

EIGHTEENTH CLAIM FOR RELIEF AND CAUSE OF ACTION
ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT
815 ILL. COMP STAT. §§ 505, *et seq.*

On Behalf of Plaintiffs Erik Brook, David Andrew, Josh Shi, Hui Li, and Debt Cleanse Group Legal Services LLC and the Illinois Subclass Against Defendant LastPass

611. Plaintiffs restate and reallege all preceding allegations in paragraphs 1 through 391 as if fully set forth herein.

612. Plaintiffs Erik Brook, David Andrew, Josh Shi, Hui Li, and Debt Cleanse ("Plaintiffs") bring this claim on behalf of themselves and the Illinois Subclass against Defendant LastPass.

613. LastPass is a "person" as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

614. Plaintiffs and Illinois Subclass Members are "consumers" as defined by 815 Ill. Comp. Stat. §§ 505/1(e).

615. LastPass's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. § 505/1(f).

616. LastPass's deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), and the Illinois Personal Information Act, 815 Ill. Comp. Stat. §§ 530/10(a), et seq, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), and the Illinois Personal Information Act, 815 Ill. Comp. Stat. §§ 530/10(a);

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), and the Illinois Personal Information Act, 815 Ill. Comp. Stat. §§ 530/10(a), et seq.

617. LastPass's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of LastPass's data security and ability to protect the confidentiality of consumers' PII.

618. LastPass intended to mislead Plaintiffs and Illinois Subclass Members and induce them to rely on its misrepresentations and omissions.

619. The above unfair and deceptive practices and acts by LastPass were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

620. LastPass acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud Act, and recklessly disregarded Plaintiffs' and Illinois Subclass Members' rights. LastPass is an industry leader in the sale of online security and has been the object of multiple security breaches dating back to at least 2011, including when a cyber attacker gained sustained access to its development environment in or around August 2022. Taken together, LastPass was

on notice that its security and privacy protections were inadequate and had remained inadequate for the last 13 years.

621. As a direct and proximate result of LastPass's unfair, unlawful, and deceptive acts and practices, Plaintiffs and Illinois Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for LastPass's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

622. Plaintiffs and Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

NINETEENTH CLAIM FOR RELIEF AND CAUSE OF ACTION
ILLINOIS DECEPTIVE TRADE PRACTICES ACT
815 ILL. COMP STAT. §§ 510/1, *et seq.*

On Behalf of Plaintiffs Erik Brook, David Andrew, Josh Shi, Hui Li, and Debt Cleanse Group Legal Services LLC and the Illinois Subclass Against Defendant LastPass

623. Plaintiffs restate and reallege all preceding allegations in paragraphs 1 through 391 as if fully set forth herein.

624. Plaintiffs Erik Brook, David Andrew, Josh Shi, Hui Li, and Debt Cleanse ("Plaintiffs") bring this claim on behalf of themselves and the Illinois Subclass against Defendant LastPass.

625. LastPass is a "person" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

626. LastPass engaged in deceptive trade practices in the conduct of its business, in violation of 815 Ill. Comp. Stat. §§ 510/2(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

627. LastPass's deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), and the Illinois Personal Information Act, 815 Ill. Comp. Stat. §§ 530/10(a), et seq., which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), and the Illinois Personal Information Act, 815 Ill. Comp. Stat. §§ 530/10(a), et seq.;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), and the Illinois Personal Information Act, 815 Ill. Comp. Stat. §§ 530/10(a), et seq.

628. LastPass's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of LastPass's data security and ability to protect the confidentiality of consumers' PII.

629. The above unfair and deceptive practices and acts by LastPass were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and Illinois Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

630. As a direct and proximate result of LastPass's unfair, unlawful, and deceptive trade practices, Plaintiffs and Illinois Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for LastPass's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

631. Plaintiffs and Illinois Subclass Members seek all relief allowed by law, including injunctive relief.

CLAIMS ON BEHALF OF THE NEW YORK SUBCLASS

TWENTIETH CLAIM FOR RELIEF AND CAUSE OF ACTION
NEW YORK GENERAL BUSINESS LAW
N.Y. GEN. BUS. LAW §§ 349, *et seq.*

On Behalf of Plaintiffs Amy Doermann, R. Andre Klein, Steven Carter and the New York Subclass Against Defendant LastPass

632. Plaintiffs restate and reallege all preceding allegations in paragraphs 1 through 391 as if fully set forth herein.

633. Plaintiffs Amy Doermann, R. Andre Klein, and Steven Carter ("Plaintiffs") bring this claim on behalf of themselves and the New York Subclass against Defendant LastPass.

634. LastPass engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs' and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

h. LastPass's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of LastPass's data security and ability to protect the confidentiality of consumers' PII.

635. LastPass acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiffs' and New York Subclass Members' rights. LastPass is an industry leader in the sale of online security and has been the object of multiple security breaches dating back to at least 2011, including when a cyber attacker gained sustained access to its development environment in or around August 2022. Taken together, LastPass was on notice that its security and privacy protections were inadequate and had remained inadequate for the last 13 years.

636. As a direct and proximate result of LastPass's deceptive and unlawful acts and practices, Plaintiffs and New York Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for LastPass's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

637. LastPass's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the many New Yorkers affected by the Data Breach.

638. The above deceptive and unlawful practices and acts by LastPass caused substantial injury to Plaintiffs and New York Subclass Members that they could not reasonably avoid.

639. Plaintiffs and New York Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE OKLAHOMA SUBCLASS

TWENTY-FIRST CLAIM FOR RELIEF AND CAUSE OF ACTION OKLAHOMA CONSUMER PROTECTION ACT OKLA. STAT. TIT. 15, §§ 751, *et seq.*

On Behalf of Plaintiff Daniel LeFebvre and the Oklahoma Subclass Against Defendant LastPass

640. Plaintiffs restate and reallege all preceding allegations in paragraphs 1 through 391 as if fully set forth herein.

641. Plaintiff Daniel LeFebvre brings this claim on behalf of himself and the Oklahoma Subclass against Defendant LastPass.

642. LastPass is a "person," as meant by Okla. Stat. tit. 15, § 752(1).

643. LastPass's advertisements, offers of sales, sales, and distribution of goods, services, and other things of value constituted "consumer transactions" as meant by Okla. Stat. tit. 15, § 752(2).

644. LastPass, in the course of its business, engaged in unlawful practices in violation of Okla. Stat. tit. 15, § 753, including the following:

a. Making false or misleading representations, knowingly or with reason to know, as to the characteristics, uses, and benefits of the subjects of its consumer transactions;

b. Representing, knowingly or with reason to know, that the subjects of its consumer transactions were of a particular standard when they were of another;

c. Advertising, knowingly or with reason to know, the subjects of its consumer transactions with intent not to sell as advertised;

d. Committing deceptive trade practices that deceived or could reasonably be expected to deceive or mislead a person to the detriment of that person as defined by section 752(13);

e. Committing unfair trade practices that offend established public policy and was immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers as defined by section 752(14).

645. LastPass's unlawful practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

646. LastPass's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of LastPass's data security and ability to protect the confidentiality of consumers' PII.

647. LastPass intended to mislead Plaintiff and Oklahoma Subclass Members and induce them to rely on its misrepresentations and omissions.

648. Had LastPass disclosed to Plaintiff and Oklahoma Subclass Members that its data systems were not secure and, thus, vulnerable to attack, LastPass would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. LastPass was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and Oklahoma Subclass Members. LastPass accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Oklahoma Subclass Members acted reasonably in relying on LastPass's misrepresentations and omissions, the truth of which they could not have discovered.

649. The above unlawful practices and acts by LastPass were immoral, unethical, oppressive, unscrupulous, and substantially injurious. These acts caused substantial injury to Plaintiff and the Oklahoma Subclass Members.

650. LastPass acted intentionally, knowingly, and maliciously to violate Oklahoma's Consumer Protection Act, and recklessly disregarded Plaintiff and Oklahoma Subclass Members' rights. LastPass is an industry leader in the sale of online security and has been the object of multiple security breaches dating back to at least 2011, including when a cyber attacker gained sustained access to its development environment in or around August 2022. Taken together, LastPass was on notice that its security and privacy protections were inadequate and had remained inadequate for the last 13 years.

651. As a direct and proximate result of LastPass's unlawful practices, Plaintiff and Oklahoma Subclass Members have suffered and will continue to suffer injury, ascertainable losses

of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for LastPass's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

652. Plaintiff and Oklahoma Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, civil penalties, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE PENNSYLVANNIA SUBCLASS

TWENTY-SECOND CLAIM FOR RELIEF AND CAUSE OF ACTION PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW 73 PA. CONS. STAT. §§ 201-1, *et seq.*

On Behalf of Plaintiff Hui Li and the Pennsylvania Subclass Against Defendant LastPass

653. Plaintiffs restate and reallege all preceding allegations in paragraphs 1 through 391 as if fully set forth herein.

654. Plaintiff Hui Li brings this claim on behalf of himself and the Pennsylvania Subclass against Defendant LastPass.

655. Plaintiff and Pennsylvania Subclass Members purchased goods and services in "trade" and "commerce," as meant by 73 Pa. Cons. Stat. § 201-2(3), primarily for personal, family, and/or household purposes.

656. LastPass engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of its trade and commerce in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including the following:

a. Representing that its goods and services have approval, characteristics, uses, or benefits that they do not have (73 Pa. Stat. Ann. § 201-2(4)(v));

b. Representing that its goods and services are of a particular standard or quality if they are another (73 Pa. Stat. Ann. § 201- 2(4)(vii)); and

c. Advertising its goods and services with intent not to sell them as advertised (73 Pa. Stat. Ann. § 201-2(4)(ix)).

657. LastPass's unfair or deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

658. LastPass's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of LastPass's data security and ability to protect the confidentiality of consumers' PII.

659. LastPass intended to mislead Plaintiff and Pennsylvania Subclass Members and induce them to rely on its misrepresentations and omissions.

660. Had LastPass disclosed to Plaintiff and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, LastPass would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. LastPass was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and Subclass Members. LastPass accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Subclass Members acted reasonably in relying on LastPass's misrepresentations and omissions, the truth of which they could not have discovered.

661. LastPass acted intentionally, knowingly, and maliciously to violate Pennsylvania Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff and Pennsylvania Subclass Members' rights. LastPass is an industry leader in the sale of online security and has been the object of multiple security breaches dating back to at least 2011, including when a cyber attacker gained sustained access to its development environment in or around August 2022. Taken together, LastPass was on notice that its security and privacy protections were inadequate and had remained inadequate for the last 13 years.

662. As a direct and proximate result of LastPass's unfair methods of competition and unfair or deceptive acts or practices and Plaintiff's and the Pennsylvania Subclass Members' reliance on them, Plaintiff and Pennsylvania Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased,

imminent risk of fraud and identity theft; loss of value of their PII; overpayment for LastPass's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

663. Plaintiff and Pennsylvania Subclass Members seek all monetary and non-monetary relief allowed by law, including, pursuant to 73 Pa. Stat. Ann. § 201-9.2, actual damages or statutory damages of $100 (whichever is greater), treble damages, attorneys' fees and costs, and any additional relief the Court deems necessary or proper.

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their Counsel to represent the nationwide Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the lax data security practices, procedures, networks, and systems that led to the unauthorized disclosure and subsequent misuse of Plaintiffs' and Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and Class Members or to mitigate further harm;

C. For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

E. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

F. For an award of punitive damages, as allowable by law;

G. For an award of attorneys' fees and costs, and any other expense, including reasonable expert witness fees;

H. Pre- and post-judgment interest on any amounts awarded; and

I. Such other and further relief as this court may deem just and proper.

IX. JURY TRIAL DEMAND

Plaintiffs hereby demand a jury trial for all claims so triable.

Date: August 4, 2023

Respectfully Submitted,

/s/ Edward Haber

* *Admitted Pro Hac Vice*
** *Pro Hac Vice Application Forthcoming*

Edward F. Haber (BBO# 215620)
Ian McLoughlin (BBO #647203)
Patrick J. Vallely (BBO# 663866)
SHAPIRO HABER & URMY LLP
One Boston Place, Suite 2600
Boston, MA 02108
Tel: (617) 439-3939
Fax: (617) 439-0134
ehaber@shulaw.com
imcloughlin@shulaw.com
pvallely@shulaw.com

Interim Liaison Counsel

Amy Keller*
James A. Ulwick*
DiCELLO LEVITT LLP
Ten North Dearborn Street, Sixth Floor
Chicago, IL 60602
Tel: (312) 214-7900
Fax: (312) 253-1443
akeller@dicellolevitt.com
julwick@dicellolevitt.com

Nathaniel L. Orenstein (BBO #664513)
Patrick T. Egan (BBO #637477)
Justin N. Saif (BBO #660679)
BERMAN TABACCO

One Liberty Square
Boston, MA 02109
Tel: (617) 542-8300
Fax: (617) 542-1194
norenstein@bermantabacco.com
pegan@bermantabacco.com
jsaif@bermantabacco.com

Christina M. Sarraf**
BERMAN TABACCO
425 California Street, Suite 2300
San Francisco, CA 94104
Tel: (415) 433-3200
Fax: (415) 433-6382
csarraf@bermantabacco.com

Nicholas A. Migliaccio*
Jason Rathod*
Bryan Faubus*
MIGLIACCIO & RATHOD LLP
412 H Street NE, Ste. 302
Washington, DC 20002
Tel: (202) 470-3520
Fax: (202) 800-2730
nmigliaccio@classlawdc.com
jrathod@classlawdc.com
bfaubus@classlawdc.com

Interim Co-Lead Counsel for the Plaintiffs

Michael R. Reese*
REESE LLP
100 West 93rd Street, 16th Floor
New York, New York 10025
Tel: (212) 643-0500
Fax: (212) 253-4272
mreese@reesellp.com

George V. Granade*
REESE LLP
8484 Wilshire Boulevard, Suite 515
Los Angeles, California 90211
Tel: (310) 393-0070
Fax: (212) 253-4272
ggranade@reesellp.com

Charles D. Moore*
REESE LLP
100 South 5th Street, Suite 1900
Minneapolis, Minnesota 55402
Tel: (212) 643-0500
Fax: (212) 253-4272
cmoore@reesellp.com

Interim Co-Lead Counsel for the California Subclass

James J. Pizzirusso*
HAUSFELD LLP
888 16th Street, N.W.
Suite 300
Washington, D.C. 20006
Tel.: (202) 540-7200
Fax: (202) 540-7201
jpizzirusso@hausfeld.com

Steven M. Nathan*
HAUSFELD LLP
33 Whitehall Street
Fourteenth Floor
New York, NY 10004
Tel.: (646) 357-1100
Fax: (212) 202-4322
snathan@hausfeld.com

Thomas A. Zimmerman, Jr.*
ZIMMERMAN LAW OFFICES, P.C.
77 W. Washington St., Ste 1220
Chicago, IL 60602
Tel: (312) 767-6463
Fax: (312) 440-4180x
tom@attorneyzim.com

Chairs of the Plaintiffs' Executive Committee

Sabita J. Soneji*
Cort T. Carlson*
TYCKO & ZAVAREEI LLP
1970 Broadway, Suite 1070
Oakland, CA 94612
Tel: (510) 254-6808

Fax: (202) 973-0950
ssoneji@tzlegal.com
ccarlson@tzlegal.com

Robert C. Schubert*
Amber L. Schubert*
SCHUBERT JONCKHEER & KOLBE LLP
2001 Union Street, Suite 200
San Francisco, CA 94123
Tel: (415) 788-4220
Fax: (415) 788-0161
rschubert@sjk.law
aschubert@sjk.law

Laura Van Note*
Cody Bolce*
COLE & VAN NOTE
555 12th Street, Suite 2100
Oakland, CA 94607
Tel: (510) 891-9800
Fax: (510) 891-7030
lvn@colevannote.com
cab@colevannote.com

Michael Kind*
KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, NV 89123
Tel: (702) 337-2322
Fax: (702) 329-5881
Email: mk@kindlaw.com

Marc E. Dann*
Brian D. Flick*
DannLaw
15000 Madison Avenue
Lakewood, OH 44107
Tel: (216) 373-0539
Fax: (216) 373-0536
notices@dannlaw.com

Francis A. Bottini, Jr.*
Albert Y. Chang*
BOTTINI & BOTTINI, INC.
7817 Ivanhoe Ave., Suite 102

La Jolla, CA 92037
Tel: (858) 914-2001
Fax: (858) 914-2002
fbottini@bottinilaw.com
achang@bottinilaw.com

Plaintiffs' Executive Committee

Counsel for the Plaintiffs

CERTIFICATE OF SERVICE

I hereby certify that I served a copy of the foregoing was served on counsel of record via the Court's CM/ECF system on August 4, 2023.

/s/ Ian J. McLoughlin
Ian J. McLoughlin